计算原理导论

Introduction to Computing Principles

天津大学　计算机科学与技术学院　刘志磊

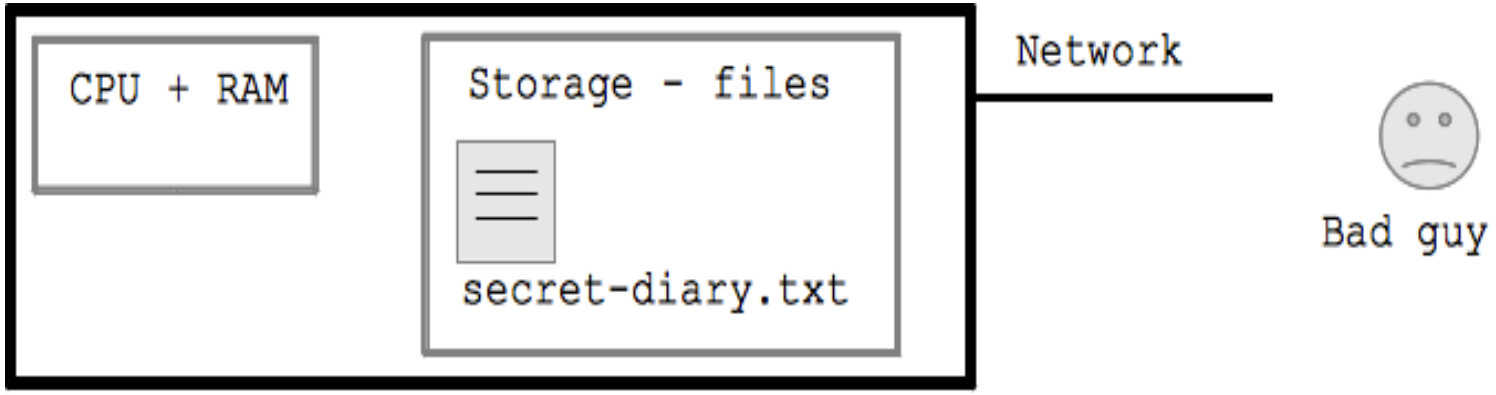
What is Computer Security?

Computer Security, also known as cybersecurity or IT security, is the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide.

-- Wikipedia

Computer -- The Castle

- The computer is like a castle with walls
- Inside and outside are very different



Computer - "castle" model

Computer Attack

In computer and computer networks, computer attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

Computer Attacks - Bulk

- Bad Guy send out millions of generic attacks, just snaring who falls for it
- "Spear phishing" refers to a specifically crafted and sophisticated attack against a specific person, but that is an uncommon case.
- If you avoid the most common errors, you will probably be fine

Bad Guy Examples

- Send Spam using your account to your address book (exploit higher trust), spam email could be just ads, or malware
- Use login on site to post spammy forum comments with links to bad stuff
- Sell fake goods on your ebay account (exploit account rating, clever!)
- Use your phone call expensive 900 numbers, money goes back to bad guy
- Turn your computer/phone into a "zombie"
- Try the same password on other accounts you might have
- Dig through your computer or steal your name, SSN etc.
- Dig through your computer for financial accounts, CC numbers
- Dig through your computer for bitcoins, super easy to steal

Bad Guy Examples - PII Broken

PII - Personal Identifying Information

Name, old addresses, SSN

These are old facts, so not easily changed like a password

PII is no longer a reliable way to authenticate that a person is who they say

Bad guys have ways to get PII cheaply on bad guy online marketplaces

e.g. ATM Card Reset

-Bad guys bulk steal ATM card stripe (name and number) but not the PIN

-Bad guys buy the person's SSN/address for a few dollars on bad guy market

-Bad guys call the bank, pose as customer, reset the PIN, then take out money

-Bad guys are resourceful! e.g. Tax Refund Fraud

-Bad guys has enough PII to submit a fake tax return, get refund

Conclusion: IRS etc. need a more reliable way to "authenticate" someone can prove it's really them

Password Attacks

- The bad guy could try to guess your password to a site. This is the "outside" case - bad guy is outside the site. Known as "dictionary attack“, as if they are trying all the words in a dictionary
- Bad guys tries to log in again and again. Bad guys will try common passwords as guesses. Works if the password is common, e.g. "password" or "password1"
- The attack fails mostly, but works some percentage of the time with an account with a weak password. As there are 86400 seconds in a day, and maybe 31 million guesses per year (1 guess/second). There is not time to make 100 billion guesses, so just avoid the weakest 10 million passwords

Password Attacks Example

```
Mar 6 06:26:20 codingbat sshd[30924]: Failed password for invalid user alex from 49.212.7.205 port 36268 ssh2
Mar 6 06:26:22 codingbat sshd[30926]: Failed password for invalid user alex from 49.212.7.205 port 36605 ssh2
Mar 6 06:26:26 codingbat sshd[30928]: Failed password for invalid user alex from 49.212.7.205 port 36937 ssh2
Mar 6 06:26:29 codingbat sshd[30930]: Failed password for invalid user adam from 49.212.7.205 port 37212 ssh2
Mar 6 06:26:32 codingbat sshd[30932]: Failed password for invalid user fax from 49.212.7.205 port 37546 ssh2
Mar 6 06:26:34 codingbat sshd[30934]: Failed password for invalid user fax from 49.212.7.205 port 37864 ssh2
Mar 6 06:26:38 codingbat sshd[30936]: Failed password for invalid user demo from 49.212.7.205 port 38201 ssh2
Mar 6 06:26:41 codingbat sshd[30938]: Failed password for invalid user demo from 49.212.7.205 port 38561 ssh2
Mar 6 06:26:44 codingbat sshd[30940]: Failed password for invalid user amanda from 49.212.7.205 port 38911 ssh2
Mar 6 06:26:47 codingbat sshd[30942]: Failed password for invalid user angie from 49.212.7.205 port 39244 ssh2
Mar 6 06:26:51 codingbat sshd[30944]: Failed password for invalid user angie from 49.212.7.205 port 39552 ssh2 ...
```

This is a real "log file" from codingbat.com server where it routinely records what happens each day. What you see here is the attacker is trying guess both the username and password on the account. They are trying common passwords, such as "secret" "password12" etc. You can see that their list of usernames to try is sort of alphabetical order, and they are just running through it in the most obvious way.

Social Engineering Attacks

Social engineering means using human to human contact, say on the phone, to get into a system. Some people can be quite persuasive on the phone, and most people are polite and helpful by default. A bad guy might pose as technician showing up, trying to fix the printer. People will often be polite to a well dressed person on site who appears to be doing something proper.

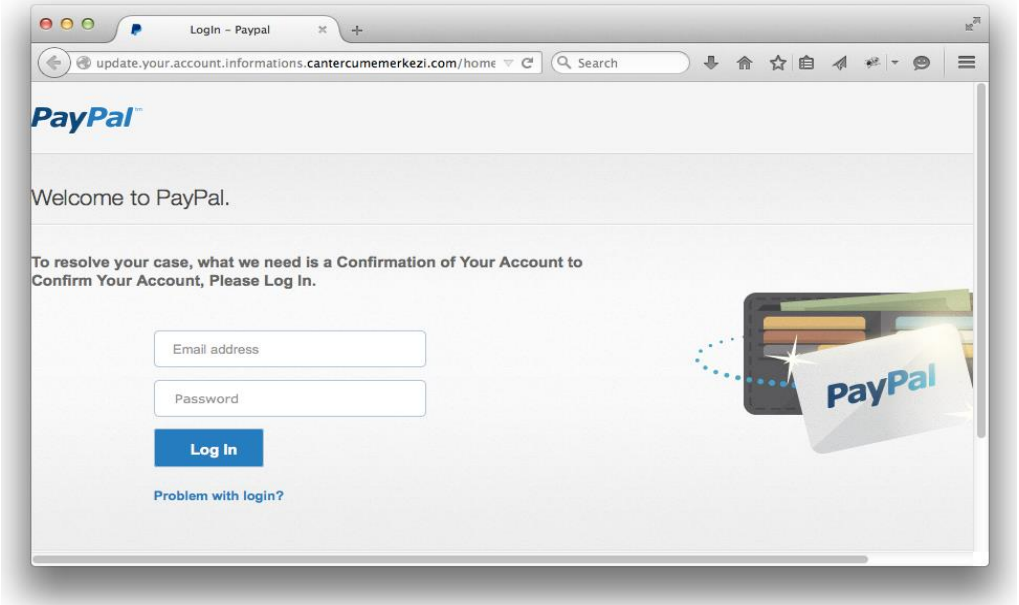
Social engineering works because people are generally helpful

Phishing Attacks

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

- "Phishing" is a type of attack where the bad guy tricks you into typing your password into a bad guy site, thus the bad guy gets your password.
- You have probably received many phishing emails. The phishing email most often includes a link to a phishing webpage.

Phishing Attacks



- The above is phishing site, not the real paypal site. If you type your username and password into the phishing site, they are sent to the bad guy who can use them to break into your account.
- The graphics and coloring are correct. Those are trivial for the bad guys to copy and mean nothing. The title of the tab - "Paypal Login" - is also meaningless.

Real Word Phishing - Fake ATM Machine

Criminals put up a fake ATM machine made of plywood in front of a real ATM, with a "under construction" sign. The victim would put their card into the fake ATM and type in their PIN. Then the machine would print an "out of order" message and give the card back. The bad guys in this way collected all the card numbers and PINs and drained the accounts over the weekend. This is a real-world analog of fake-site phishing.

Malware Attacks

Malware attacks is a big category, where the bad guy tricks the victim into running bad software ("malware") on the victim's computer. The bad softwares include viruses, worms, and trojans.

Suppose a bad guy emails you the following sort of file:

- A plain .TXT file, which you open and read on your computer
- A .JPG file, which you then open and look at on your computer
- A program .EXE file -- a program or "app" - copy on to your computer and run it
- A .DOC document file which you then open and read on your computer

How do you feel about different files?

Malware Attacks

Passive Content = Safe, Program = Unsafe

If the bad guy gets you to run bad guy authored code on your computer, the computer is compromised, the bad guy has won. The code can take actions and it's inside the computer. Recall the "castle" analogy - the bad guy program is running inside the castle.

So we trust passive content (.TXT .JPG) but not active programs (.DOC .EXE). Unfortunately, many seemingly passive formats, such as .DOC, can have "program" type qualities in them as an advanced feature, e.g. .DOC can be unsafe because of Microsoft Visual Basic macros embedded. This used to be a huge source of problems (search for "macro virus").

Malware Attacks - Trojan

A "trojan" is malware disguised as something else. The trojan tries to look like harmless content, not a program. The trojan claims to be a program that does something many people want, but really it's malware

In order to be safe from Trojan:

- Operating systems may have helpful warning "this is a program you downloaded, do you want to run it?"
- Don't run programs from random sources
- Google the name/domain-name of it first, see what people say. If something is from a well known domain and has lots of downloads, I figure someone would have flagged it if it was malware

Malware Attacks - Vulnerability

A "vulnerability" is one scary cases. If the user browses over to a web site this is hosting the "attack" content and their browser is vulnerable, then the bad guy can get it just from that. The bad guy can make the web site appear attractive, post links on reddit or whatever to try to drive traffic to the site. This attack is scary because it does not require the user to do anything especially foolish.

In order to be safe from vulnerability:

- Be sure to run the most up to date, current version of your browser and any plugins such as Flash. Firefox
- Switch to make programs auto-check for new versions, so the user does not need to do much to have the most recent version.

Malware Example - Keylogger

- Keylogger is a good example piece of malware, it is running on your computer
- Keylogger watches the screen, what urls you visit, records all the keystrokes
- HTTPS is no help - it's inside the castle
- Sends this info back to the bad guy
- Easy to imagine how this could allow the bad guy to abuse your accounts
- **Important:** do not log into your email account from some random internet-cafe machine!

Malware Example - Zombie Botnets

- A group of machines with malware on them allowing "bot herder" to control them

How to obtain the zombies?

- Bot herder sends out million emails pointing to a site that attacks a Flash vulnerability, installing the malware onto vulnerable machines
- The bot herder sends out commands for all the zombies to do something
- Botnets can be rented, there's an active botnet market in the bad-guy community (suggested interesting B-School research direction)

Malware Example - Encryption "Ransomware"

- Malware encrypts with a random password all the files on the victim machine, deletes the originals
- The victim must send the bad guys money (bitcoin) to get the "unencrypt" password
- The bad guys typically do send the password when given the money
- The scheme depends on the bad guys having a reputation of reliability
- Have backups of your important files!

Malware Example - DDOS Attack

- "Distributed Denial of Service" DDOS attack
- Attackers coordinates a large number of machines to send many requests to a site all at once
- Overwhelm the site's connection to the internet with so many packets, it becomes effectively unreachable
- When bad guys "take down" a web site in the news, typically this means a DDOS attack done with zombie machines
- **Technical** fix many DDOS techniques depend on sending packets with a forged ("spoofed") From: IP address field. The router upstream of the attacking zombie could block such forged packets from leaving their network to help blunt DDOS attacks. Nobody is very motivated to do this currently. If I were dictator of the internet, I would require it to reduce this silly pollution. (This is a tragedy of the commons.)

Malware Example - CEO Payment Email Scam

- Get email password of finance manager at company (guessing, phishing or keylogger)
- Study past emails about making wire transfers
- Study when the CEO is traveling
- Send an email like this: “Hi Bob, Im' traveling, to grab this deal, I need you to wire $25,000 to 11243-4732626 ASAP“
- May break into CEO's account to send, it or just make it look like from CEO
- Not a bulk targeted attack, bad guy effort required
- Bad guys at times have placed voice calls, pretending to be people
- Works because email about wiring money is the common practice
- Solution: have some other channel to verify, e.g. call the CEO

Password Safety

Here are some startegies to make password safety

- Avoiding the bad guy guessing or obtaining your password
- Don't use a weak password for an important site (e.g. bank, email). Email is especially important because of password-reset
- Don't re-use passwords across important sites. Bad guys have software to re-try username/passwords across a zillion sites
- Don't type in your password on some random machine in a cafe (it could have a keylogger). Cheap wi-fi phones are great for this case (e.g. Nick Starbucks example)
- Do write your passwords down, consider 2-factor authentication for important sites. Not all sites are important! Your time is valuable too.

Password Safety Practices - Good Passwords

Good Passwords

- Passwords do not need to be super elaborate to be secure
- What makes a password stronger:

  - longer
  - more characters: lower case, upper case, digits, punctuation
  - not a word or pun
- Here is what to do for secure passwords, e.g a bank site
  - Start with a word, say "kittens"
  - Change it with a random misspelling, then add some random stuff

    - kottens4x -- simple but fine password
    - not a word, not a pun, not digit-at-end
  - Here are stronger versions

    - kottens,erx -- better
    - Kottens,9erx -- better
    - KottensX,97erx -- probably more complex than necessary

Password Safety Practices - Bad Passwords

Bad Passwords

- Passwords should not be a plain word. Like ‘kittens’
- Passwords should not be too short - 6 characters is marginal, longer is better
- Passwords with only lowercase letters are weaker
  - upper case, digits, punctuation are all stronger
- Passwords should not be a pun or pattern that someone else would think of.
  - Like ‘opensesame’, ‘qwerty123’, ‘catfish’, ‘remaincalmandcarryon’
    - these sorts of passwords are on the common password list
    - When asked to make a random, memorable password, the pun instinct is strong!
- When required to add a digit to a password, many people just add 1 at the end

Password Safety Practices - What to do

- Avoid weak passwords
- Don't have to go crazy with it
- Bad guys are probably guessing thousands, not billions on you
  - e.g. kottens4x is not terrible
- Don't re-use passwords across sites
- Do consider writing down important passwords
- Not all passwords need to be super secure
- Email password is extra important, due to password re-sets
- 1 scheme: memorize suffix "x23" for passwords
- Write down passwords but not the suffix

Password Safety Practices - Two-Factor Authentication

- A second piece of information to log in, a "second factor“aka "Multi-Factor Authentication"
- Password is 1 pice of info
- Require 2nd info to log in
  - example 1: The site texts a little number to the user's registered cell phone
  - example 2: The user has a free One Time Password (OTP) app on their phone
  - example 3: U2F (below)
- Two-factor makes it much more difficult for the bad guy although not impossible
- Great side effect: with two-factor, perhaps the password can be simple "kitten2"
- Ideally, 2nd-factor not required every time
  - maybe once a month or from a new computer
- Two-factor may still fail for phishing (not U2F though)

Password Safety Practices - U2F

U2F - universal two-factor

- Device is better than passwords in our heads
- The world will not continue to use passwords as we know them today
- The new free and open Fido U2F "universal two-factor" shows a next-gen solution
- Right now works in Chrome
- It's an inexpensive little device you can carry around, it has one button on it
- You click a button on the device when asked to prove you are you, and the rest is automatic
- Secure and convenient - you don't have to type anything.
- Ultimately your phone will work as a U2F token too
- It is also phishing proof - click the button on a "bad guy" site and there's no harm
- U2F is so secure, the password can be trivial, like 4 digit PIN or perhaps nothing

Phishing Safety

- Avoiding the bad guy tricking you into disclosing your password
- Something is asking for your password? Look up at the browser url area
- Something is asking for your password? Look up at the browser url area
- Something is asking for your password? Look up at the browser url area
- Watch out for clever bad guy urls: weblogin.stanford.edu-xnr-xyzldlwerou.ru
- Proceed carefully with content from email or random pages with provocative "click this" content
- Or just type in "www.schwab.com" yourself in the browser instead of clicking in the email - super simple and secure practice
- U2F Two Factor - solves both password and phishing problems, a technical fix

Phishing Safety Practices - Avoiding Phishing

- Don't trust urls in emails or sites when they lead to a login page
- The bad guy is hoping that when the username/password fields appear in front of you, you will just type it in out of a habit. When asked for your password, slow down for a moment and look.
- Technique 1: Scrutinize the url near the top of the browser window
- The bad guy url will try to look legitimate but it is not the correct url, e.g. www.ebay.bad-guy.ru is not the official ebay site, which should end in "ebay.com"
- Technique 2: (more secure) Type the url into your browser yourself -- if the email claims you need to log into ebay, go to your browser manually and type in "www.ebay.com".
- Chrome and the other major browsers have an ongoing effort to detect and warn users about phishing sites in realtime. If you see a phishing site, you can use the "report web forgery" menu item in our browser to report the site, contributing against the bad guys.
- Look for https in the url

Phishing Safety Practices - HTTPS

HTTPS: "secure" variant of HTTP to transfer web page over the internet

HTTPS does two things:

1. HTTPS requires some paperwork to set up, so that the domain www.schwab.com domain name really is coming from the Schwab organization.
   -Helps prevent phishing, but the user still needs to look at the url
   -e.g. Checking that it's www.schwab.com not www.schwarb.bad-guy.ru
2. HTTPS encrypts all the traffic, so interception of the bytes does not yield anything intelligible

Phishing Safety Practices - Encryption

- "Encryption" is a way of scrambling data before it is sent out in packets, so that even if intercepted, they are meaningless
- HTTPS provides encryption, in addition to its url-verification feature
- No one on the internet can get my password out of the encrypted package? Because HTTPS encrypted all the packets before they were sent out.
- Note if the machine had malware on it, it could steal the password as typed it in.
- HTTPS only takes care of the networking.

Malware Safety

- Avoiding the bad guy installing software on your machine
- Trojan - be wary of downloading and running an application
- Trojan - be wary of .zip file in email
  -like phishing, what domain is hosting this thing I'm downloading?
  -google the name of the site. If it has lots of complaints?
- Trojans are commonly sent in email, often in a .zip file
- Phones best to install apps from official apple/google stores only
- Vulnerability case - keep internet-facing software on auto-update to stay at the latest

Malware Safety Practices – Phone vs. Malware

- Traditional computer -- installed application can do anything, general purpose
- Phone model -- applications and what the user can do is more limited and isolated
- Adding limits has some advantages
- In the limited phone environment, each application is "sandboxed" can only do some things
- Android: user sees list of specific, limited capabilities at install time
- Apple: there's an Apple review process
- Both android and Apple have had malware, with Android currently showing more
- Google and Apple can remotely disable software once it's discovered to be malware
- Google/Apple stores have anti-malware, detecting bad stuff -use the official stores
- There's an arms-race here between google/apple and the bad guys
- I hope that Google/apple may ultimately be able to lock things down
- Ultimately: limit applications so the phone is still usable and trustable no matter what the user does, limiting/managing the applications to prevent harm

Private Key Cryptography

Symmetric-key cryptography uses the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption (also known as asymmetric key encryption).

Private Key Cryptography

- Current tech: the "AES" standard, mature, reliable, widely used
- It is thought that no government has "broken" AES

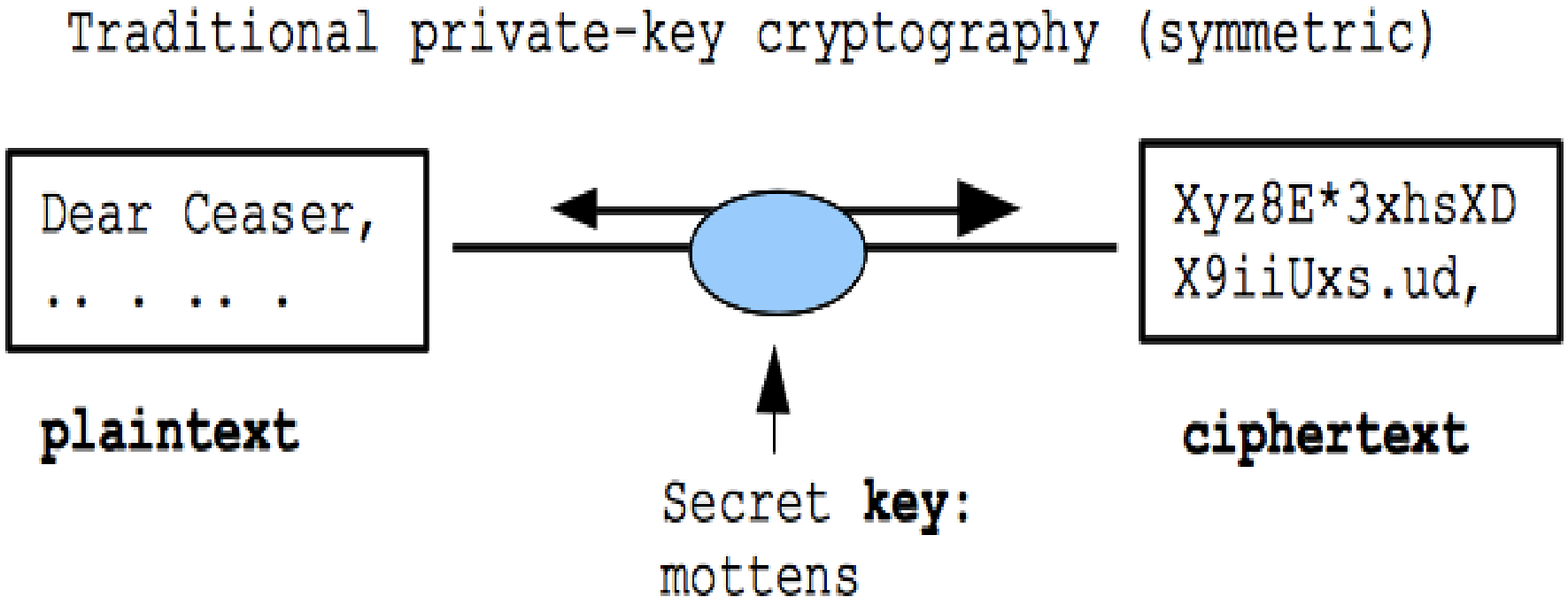
Two results one obvious, one subtle:

1. secrecy attacker intercepts the ciphertext, but cannot recover the plaintext from it
2. authenticity attacker cannot "spoof" data, sent to be decrypted. If the ciphertext decrypts cleanly, it must have come from a party with the secret key

The only "attack" known is "brute force" which try to guess through the space of all possible keys (if the original key is long, it's safe)
Note: any encryption can be attacked brute force, so if that's the best attack known, the encryption is regarded as un-broken

Problem: key distribution. How do you share the key securely between parties?

Private Key Cryptography



Private Key Application - File/Disk Encryption

One day, your laptop is going to get stolen. Suppose you have a spreadsheet on their with people's SSNs? Suppose your browser is already logged in to important sites. Most likely, the thief just wants to sell your laptop, but naturally you're a little worried about your information

- Approach 1: Encrypt a sensitive file, deleting the original
- Approach 2: set up whole-disk encryption on the laptop (or whole-disk encryption)

Disk encryption:

- a big random key is created automatically
- the whole file system is encrypted with it
- your typed password encrypts/decrypts that key

Private Key Application - File/Disk Encryption

Machine wakes: your password unlocks the key to decrypt all the files
No password, no files!
The files in your home directory are all stored in encrypted form .. docs, browser prefs, everything

Good: thief gets your laptop but no files.
Problem: annoying to type in your password
Problem: if you forget the password, your data is truly inaccessible - AES is not broken!

Still, this is a pretty good solution (Stanford staff are supposed to enable disk-encryption)
The "ransomware" malware uses symmetric encryption - the malware encrypts your files, you send the bad guys money, they send you the key to decrypt your files

Private Key Application - Phone Encryption

- San Bernardino Terrorists
- FBI had their phone
- Phone used whole-disk encryption
- It was in a state where 10 wrong PIN entries would delete all the files
- The FBI took apart the phone and with great effort recovered the PIN anyway
- There was a good chance that they would not have been successful (50%?)
- Point 1: encryption pretty much works
- Point 2: With huge budget/effort, a govt may find a way around

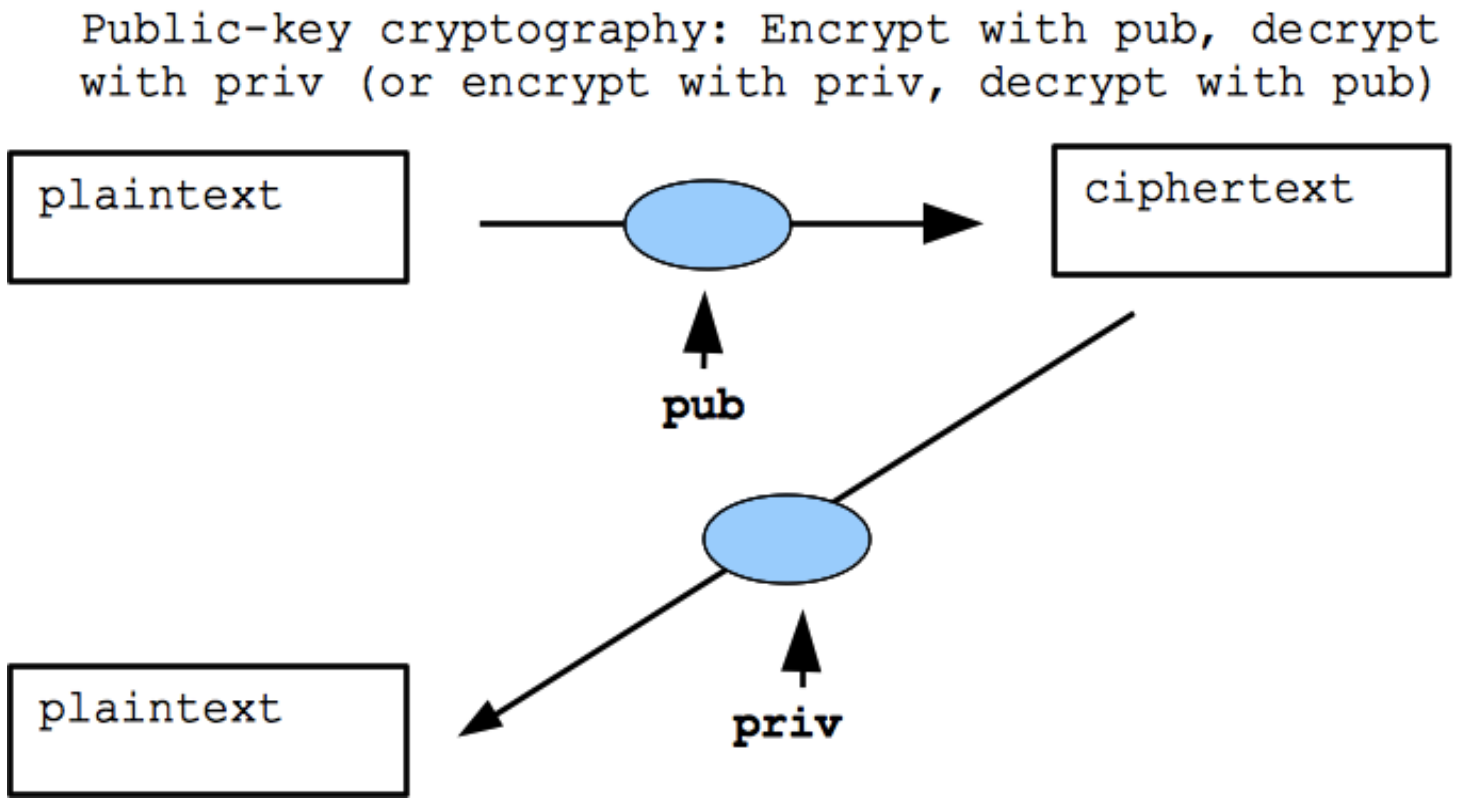
Public Key Cryptography

Public-key cryptography, or asymmetric cryptography, is any cryptographic system that uses pairs of keys: public keys that may be disseminated widely paired with private keys which are known only to the owner. There are two functions that can be achieved: using a public key to authenticate that a message originated with a holder of the paired private key; or encrypting a message with a public key to ensure that only the holder of the paired private key can decrypt it.

Public Key Cryptography

- Public-key cryptography ("asymmetric")
- Amazing technology, surprising that it is even possible
- Used on the internet all the time

Public Key Cryptography



Public Key Cryptography

Instead of a simple key used in private key cryptography, the key is created with two parts: public and private

Your computer can just make up a public/private key pair out of thin air based on random numbers

Key features:

1. The public/private keys work as encryption opposites of each other: encrypt with public key, and decrypt with private key, Or encrypt with private key and decrypt with public key.
2. If someone knows public key, they cannot easily compute private key from it. This is an impressive feature, given how closely public/private must be related to work as opposites.

Public Key Application - Packet Secrecy

1. Suppose www.example.com wants to accept packets from anyone, but so they are secret from eavesdropping
2. www.example.com makes up a public/private key pair
3. www.example.com publishes the public part of the pair so everyone can see it. Private is kept inside www.example.com.
4. Someone who wants to send a packet to www.example.com first encrypts it with public key
5. At www.example.com the encrypted packet is decrypted with private key

Provides: no key exchange problem!
HTTPS is built on something like structure - that's how your browser does the encryption with HTTPS sites

Public Key Application - Digital Signatures

- Another amazing feature enabled by public key cryptography
- A party can make up a public/private key pair as usual
- Use their private key to "sign" a file, distribute that signature
- The signature is not forgeable without the private key
- Another party can look at the signature and verify that it is valid

Governments vs. The Internet

Free speech and freedom:

Beware of he who would deny you access to information, for in his heart he dreams himself your master.

-- Sid Meier

You have the right to remain silent. Anything you say can and will be used against you in a court of law. You have the right to talk to a lawyer and have him present while you are questioned. If you cannot afford to hire a lawyer, one will be appointed to represent you before questioning, if you wish one.

-- Miranda rights

Governments vs. The Internet

Major trends of Governments vs. The Internet:

- Government Surveillance
  - Snowden disclosures
  - NSA spying on everybody
  - How much?
  - 2 scenarios are clear, 1 unknown

- Governments vs. Free Speech

Governments Surveillance - Motivated Spying

- Say a government/agency is highly motivated to spy on a particular person, e.g. Government trying to prosecute a Mafia type conspiracy
  In this case, the attacker can likely get all sorts of info (mostly legally):
  1. Warrant -- they could get warrant for email records, phone records, wiretaps, ...
  2. They could physically break in and install a keylogger on a laptop or gadget on a car ...
  3. They could exploit an unknown vulnerability to install malware on a particular person's machine (China and the NSA are accused of this)
- "Spear Phishing" .. like phishing, but crafted for just that person, e.g. send a specially crafted email trojan to a particular person

Summary: for a motivated, well financed attacker, the attack is probably successful
With a warrant, it's legal too

Governments Surveillance - Motivated Encryption

Encryption is reliable, e.g. AES encryption. If someone encrypts a hard drive or file with a good password, it's unbreakable so long as the password is nice and long
e.g. Child Porn encrypted hard drive (http://www.wired.com/2013/08/feds-crack-encrypted-drives/). For months the government could not crack/guess the password, ‘child porn‘

If the password was, say, twice as long, it would never have been cracked
Doubling password length squares the space of possible passwords
Interesting edge case in the law:

- Can a suspect be required to divulge a password?
- Can a suspect be required to give a PIN or fingerprint?

Those are not yet settled 5th-amendment issues in the US:
Can a suspect be forced to reveal a password/PIN under probable cause

Governments Surveillance

The US government does not have the resources to monitor everything going on on the internet. But they could be monitoring some things in coarse detail (Snowden revelations)

- e.g. who calls who (which numbers call which numbers, not the audio)
- e.g. who visits certain web sites

1. Is that legal without a specific warrant?
2. How much are they doing? Nobody is sure, but it's some -- the Snowden disclosure
3. It looks like the US Government was collecting information without a warrant
4. The level of surveillance was too high - illegal

Governments vs. Free Speech

- Autocracies are against sharing ideas: free speech, opinions, blogs, newspapers, twitter
- Reasons for hope:
  1. Fall of communism: VHS video tapes showing western life overpowered the 24/7 regime propaganda (Francis Fukuyama, Stanford)
  2. Fukuyama in a nutshell: people can tell when they're being lied to all the time, they deeply dislike it, and this dislike cannot be erased, no matter how voluminous the propaganda
  3. Neal Stephenson story about Miranda rights
  4. China, dictatorships etc. strongly against free speech
  5. Being critical of your own institutions is an important value
  6. The US Government has many flaws
  7. The US Government is extremely good on freedom of speech

How Governments Censor Free Speech

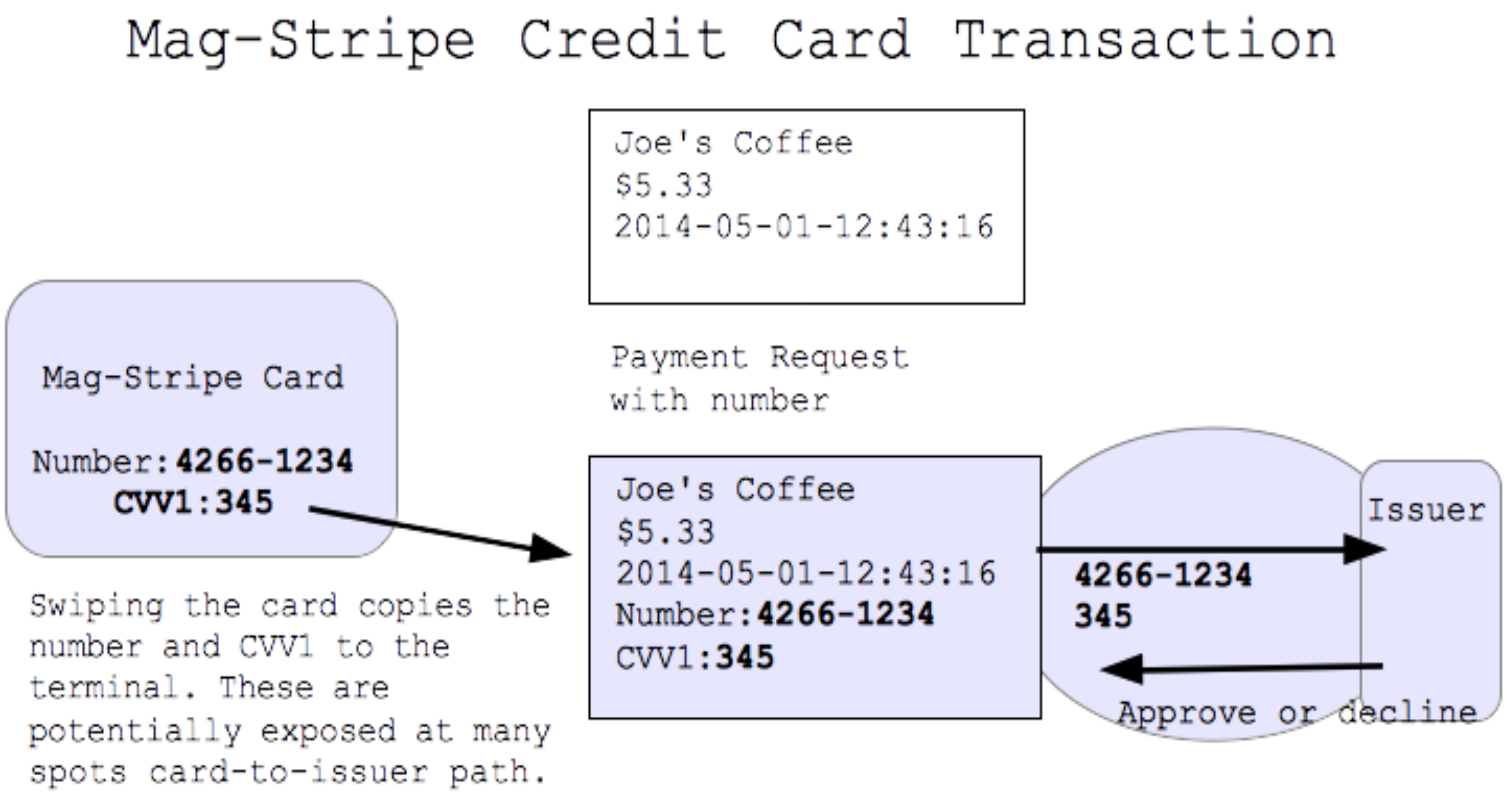
- China, North Korea: traditional autocratic, what the people are allowed to say / read
- Pakistan, Saudi Arabia: mixing in limitations on un-islamic thought, combined with autocracy
- Control TCP/IP routers the connect country to whole internet
- Block certain IP addresses, domain names
- China has an army of people who monitor blogs etc., delete ideas that are not officially permitted
- China also has an army that floods the forums etc. with government-view posts
- What "Tiananmen" search looks like with censorship inside China
- A report from Washington Post shows that Censorship Works (https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html)
- Some video materials are blocked in China
- This all seems like a tragic error that's going to hold China back
- Free speech has great value, China's censorship looks insane
- The censorship has the appearance of a kleptocracy, just trying to keep out-of-power people in the dark
- Hope: email, twitter, video ... increasing ease of information sharing making it harder to suppress the truth, per Francis Fukuyama

EMV (Europay Mastercard Visa) Cards

- EMV Card, aka Chip Card, have been in use in Europe for over 20 years
- EMV Cards also Known as "Chip and Pin" or "Chip and Signature" cards
- EMV is much more secure than old mag-stripe
- The details are complicated, but the basics are simple

EMV Cards vs. Mag-Stripe Credit Cards

How Do Mag-Stripe Credit Cards Work?



EMV Cards vs. Mag-Stripe Credit Cards

How Do Mag-Stripe Credit Cards Work?

- The old way - really quite insecure
- One "secret" is the Credit Card number, printed on the front of the card
- There's also a "CVV1" number on the mag stripe, not printed on the back
- Anyone who has these "secrets" can try making charges
- There is a different CVV2 number printed on the back
- Card-swipe: "secret" is the CC number + CVV1

EMV Cards vs. Mag-Stripe Credit Cards

Mag-Stripe Credit Cards Weaknesses

Weakness: the "secret" can be stolen along the whole path

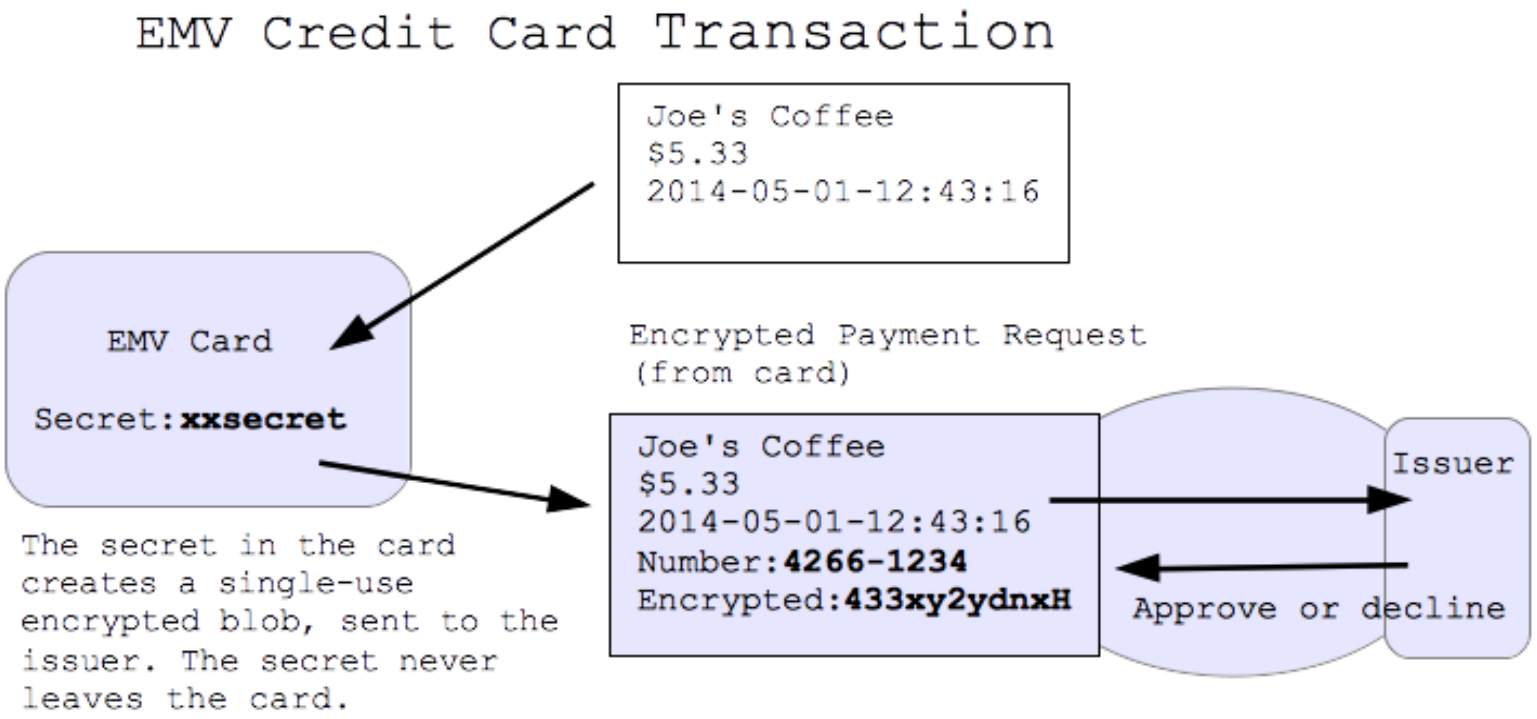
1. in the magstripe reader ("skimmer")
2. in the POS (Point of Sale) device. Target POS breach, 40 million cards
3. the waiter covertly swipes it to get the secret
4. along the path to the issuing bank

Example: A "skimmer" bad guy device attached to ATM, steals "secret“, e.g. Krebs Skimmer (http://krebsonsecurity.com/2010/01/would-you-have-spotted-the-fraud/)

Conclusion: sending the "secret" unencrypted is a terrible system. There are many places the bad guys can get to it

EMV Cards

How EMV works



EMV Cards

How EMV works

•Insert the card chip-side up into the terminal
•Leave the card inserted, so it can communicate
•Merchant creates a payment request, sends it into the card
•The chip in the card creates with its secret an encrypted "blob" request
    -e.g. imagine the card encrypts the request with the secret key
•Merchant sends the encrypted blob to the issuer to request payment
•The issuer has a copy of the secret to decrypt the request
•Key improvement: Encrypted blob is useless to the bad guys if intercepted
•The secret never leaves the chip
•The secret is what one needs to make encrypted blobs
•Avoid needing 100% security along the card-to-issuer path
•The request includes the CC number but not the needed CVV1

EMV Cards

Contactless

The little wireless-pay terminals
There are based on EMV too
Apple Pay, Google Pay, etc.
Retain the key feature: data interception is harmless

Card Shift

Mag stripe: anyone holding the card can get the info off it
-Bad guy makes a duplicate card, goes to Best Buy etc.
EMV: only the chip in the card can make a valid request
-Having the card briefly does not allow one to make a duplicate
Therefore: the bad guys must steal the physical card

EMV Weakness

Card Stolen

- The physical card itself is vital
- Bad guy could steal it from your wallet, go use it
- Some EMV cards require a PIN, guarding against the card-stolen case
- In the US, issuers are choosing to not do PIN
- My guess: skimming was a big problem, card-stolen is relatively rare
- US issuers may add PIN back, once people are used to EMV

On The Internet

Typing your CC number on a web site is CNP (Card Not Present)
CNP is not getting the benefit of the EMV chip
When Europe introduced EMV, CNP fraud went up!
Maybe cell phones will supplant cards eventually
Basic agency problem: the merchants eat the loss for CNP fraud
-But the issuers control the tech .. lack motivation
The issuers eat the fraud for "skimming" fraud

EMV Summary

- This is going to be a big improvement
- Makes the skimming (Target) case disappear
- There are weaknesses, but not fatal ones
- We might see PIN get rolled out in the USA eventually
- Next we need to solve the CNP "internet" case

Thank You!

Q&A