Security Considerations

RFC 3552 – Guidelines for Writing RFC Text on Security Considerations

Security Directorate is Working on RFC 3552 Update

- The foundations in 3552 are still good
  - Goals
    - Communication Security
    - Non-Repudiation
    - Systems Security
  - Active vs. Passive attacks
- Updates
  - Pervasive passive monitoring
  - Updated crypto
  - But progress is currently stalled

Attack Phases

- Lockheed Martin – The Cyber Kill Chain® / SecureWorks Kill Chain

1. Reconnaissance
2. *Development*
3. Weaponization
4. Delivery
5. Exploitation
6. Installation
7. Command and Control
8. Action on Objectives

http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html
https://www.secureworks.com/resources/wp-breaking-the-kill-chain

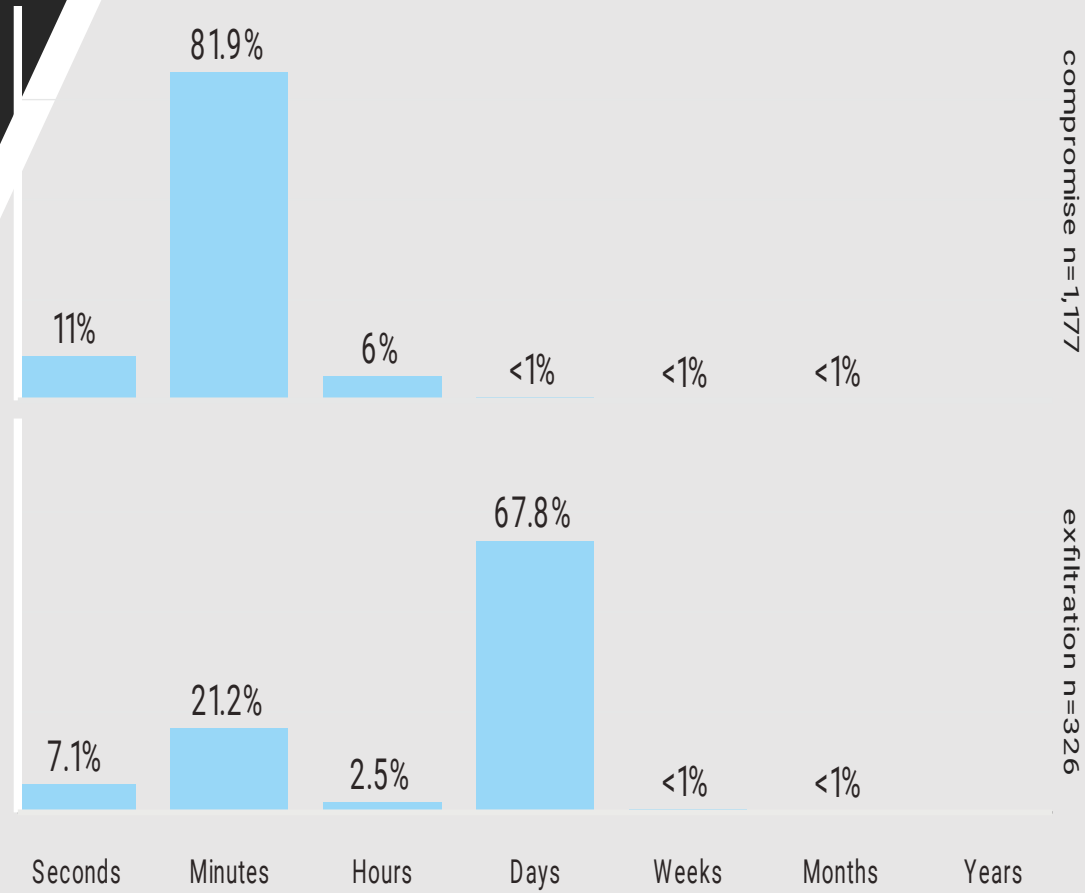
Another Attack Model

- The Lockheed Martin (or SecureWorks adaptation) model presumes an adversary intent on persistence
  - Wants to stay and observe/disrupt your compute system

- Maybe not a “simple” cyber criminal

Verizon Data Breach Report 2016

- Maybe persistence isn't necessary
- Data indicates that "smash and grab" is a viable model too



http://www.verizonenterprise.com/verizon-insights-lab/dbir/

And Pervasive Passive

- Metadata collection on a significant portion of Internet conversations
- Being able to monitor large scale Internet backbone links
  - Especially at critical peering points

- A different kind of attack against privacy

Passive vs. Active Attackers

- Passive attacker
  - Can see all packets exchanged outside of the **defined security border**
  - Can build comprehensive behavioral model of communications
  - Can do offline analysis/attacks against collected data

- Active attacker
  - Can inject packets into the network
  - Might be able to modify packets between parties in the network
  - Packet injection points may be limited or unlimited – state your assumption

Security Considerations Impacts

- Helping the security reviewer with understanding your draft
  - A concise description of what problem your draft addresses
  - The environment in which your proposed solution will operate in

- Developing the attack scenario at the beginning of the security considerations
  - Passive attacker threats / active attacker threats
  - Information protection / describing the security boundary
  - What attacks apply / which attacks do NOT apply **and** why

Considerations Agenda

- Communication Security (Data collection / Information Leakage)
- Soft middle networks
- DNS – (rendezvous protocols)
- Internet of Things
  - Denial of Service
  - Amplification Attacks
- Phishing
  - Malicious attachments
  - Infected Web Sites

Communication Security

- Passive attacks collect significant amounts of information
  - Humans are creatures of habit
    - Arrive at the office and check their favorite websites and email every morning around the same time of day
  - Metadata about network connections can reveal quite a bit of information
    - Not everything on the internet is just reading today's news
- Really smart passive collection is enhanced with minimal packet inspection / active inspection
  - Determining network defense appliances via header inspection / certificates
  - Understanding carrier packet manipulation (middle boxes) via targetted probes

Communication Security

- Create security boundaries inside protocols to ensure confidentiality
  - Ensure that the minimum amount of data is used to create a security exchange
  - Leverage secure protocol layering as soon as is practical
- Work to ensure behavioral and side channel attacks against protocol are minimized
  - Even with encryption, behavioral analysis and possible side channel attacks on protocol behavior may leak information

Security Considerations Impacts

- Communications integrity and confidentiality need to both be ensured
- Protocols/systems that are designed as middleboxes need to be mindful of impacts to other protocols assumptions
- Must assume that the network (unintentionally malicious or not) may interfere with the end-to-end principle
  - Will cellular network operators optimizations expose detailed customer end point configuration by traffic manipulation/optimization?
- Minimize in-the-clear information exchange if needed at all
- Be mindful of side-channel information leakage

Soft Middle Networks

- Soft Middle Network – all security and protections are provisioned at the perimeter of the network; inside the perimeter there is a high level of trust and a minimal amount of segmentation

Soft Middle Networks

- Network security of this design implies that finding a vulnerability in the perimeter is catastrophic to overall system security
- Once a toehold is achieved in the network, lateral movement within the network in unimpeded

- Keeping separate authorization domains can help delay access to internal network resources
- Understanding trust relationships established between devices/protocols to minimize impact

Security Considerations Impact

- Understand and state trust relationships
- Understand basic and enterprise level authentication mechanisms
- Employ least privilege into the design of protocols and systems as possible

DNS

- A rendezvous protocol: a protocol that lets other protocols determine where to connect – where other protocols should rendezvous
- The name translation protocol from human names into network endpoint identifiers (machine names)
- The Internet’s distributed database
  - Holds SRV records on your LAN
  - X.509 certificates use DNS Fully Qualified Domain Names (FQDN) as their unique keys

DNS Attacks

- Active attacks against the operation of DNS
  - Kaminsky cache poisoning attack
  - Cache poison attack via race condition
- Passive observation
  - Observing DNS requests for passive understanding
    - E.g. `read.amazon.com` – when a computer resolves that, someone probably wants to read (in that case their kindle library)
    - *.mcafee.com – likely running McAfee as their Antivirus tool, especially if you see it on a periodic update basis
  - Trending and behavioral analysis of entities based on their DNS behavior
  - Watching for SRV record requests when machines leave “home”
- If an attacker can poison the lookups, then MITM attack against many protocols, including TLS becomes possible
  - Maybe everyone should use DNSSEC

Security Considerations Implications

- Important to understand using DNS as an identity anchor in protocol development
  - Should take into account risks and many of the existing mitigations
    - DNSSEC with a validating client
    - DNS over TLS (RFC7858)
  - Understand the information leakage when doing a lookup
  - Understand the trust relationship between a local caching recursive resolver and the DNS roots

Routing

- BGP – Border Gateway Protocol
  - Autonomous Systems (AS) advertise network prefixes
  - An AS advertises the network prefixes that it serves
  - An AS can additionally relay other prefixes it sees

- But this can allow advertisements of network prefixes that aren’t your own
  - Maybe a mistake
  - Maybe intentional and malicious
  - Maybe intentional and convenient
    - Might just be trying to save table space and advertising a slightly larger space
    - Then forwarding the extra packets along– just like your ISP

Routing

- A handful of fun routing events
  - Feb 2008 – Pakistan attempts block Youtube, but advertises prefix globally, takes Youtube down
  - April 2010 – China Telecom sends out 37,000 prefixes in 15 minutes hijacking large parts of the Internet through China
  - Feb 2014 – Canadian ISP used to redirect traffic from ISPs to steal Bitcoin
- Can prevent a lot of this with BGPSEC
  - Unfortunately, adoption is still at ~6.5%
- Filtering can prevent a lot of badness too

https://en.wikipedia.org/wiki/BGP_hijacking
https://rpki-monitor.antd.nist.gov

Security Considerations Implications

- Networks and network connectivity can be hijacked or black holed via routing
- Routing impacts can be global or regional
- Combining routing attacks with other attack types can make them more powerful
- Can be used for denial of service
- Drafts should ensure their trust anchors are durable to such infrastructure attacks

Internet of Things

- Manufacturers, PLEASE follow basic security engineering
  - No non-disablable backdoors
  - No default passwords
  - Use a modern up-to-date and patched OS image
  - Do secure (signed) image software updates
  - Use crypto wisely

Denial of Service Amplification Attacks

- If we put enough completely insecure IoT devices then no one will be able to withstand the ensuing DDoS attacks

- Careful about naturally asymmetric protocols
  - Small queries with large responses allow asymmetric network behavior
    - See DNS and NTP
  - If an attacker can forge the end-point address, then can leverage public Internet services to amplify network bandwidth

Security Considerations Implications

- IETF is doing a lot of good work on IoT management and security
  - ACE, ACME, HIP, HOMENET, SAVI, JOSE

- A lot of guidance from non-IETF sources
  - Too many to list, see **draft-ietf-opsec-efforts-20.txt**

Other

What NOT to do

- Do not invent a completely new security mechanism unless you REALLY REALLY have to
  - And then think twice about doing it
- Do not reuse security terms for new purposes in your drafts
  - Redefining NONCE is not a good idea

What to do

- Ask for help with crypto – the Crypto Forum can help
- Make crypto upgradeable without having to submit a BIS protocol
  - IANA code points can be really useful
- Think about security early – please
- Consider what you will consider your boundary
- Leverage existing STD track security mechanisms
- Ask for help if you need it

Backups

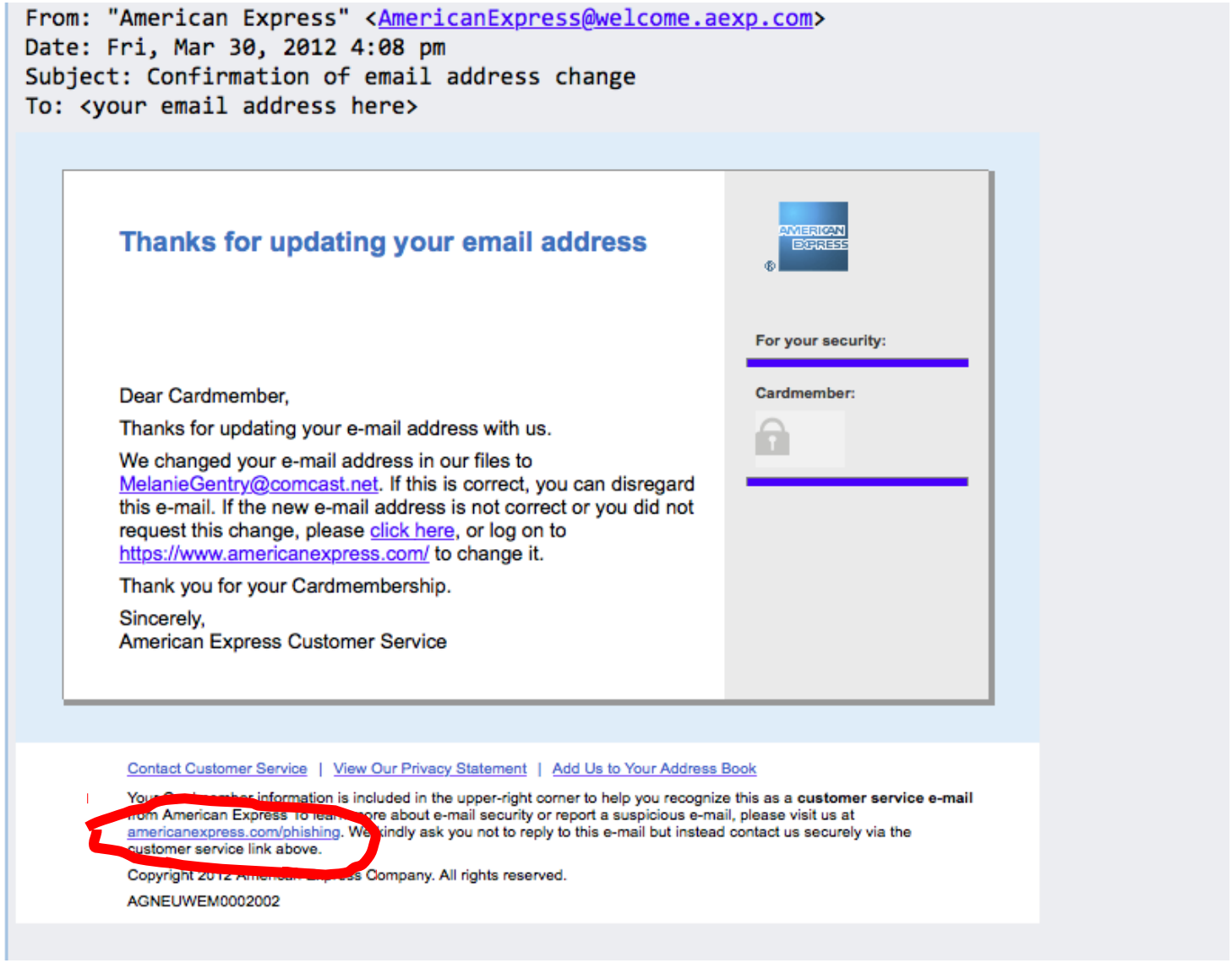
Phishing

- Not really a security considerations section BUT

- Phishing – because it still works!
  - Highly targeted phish emails may be almost impossible to tell from valid emails
  - Don’t fall for it
  - PLEASE don’t click on the link
  - PLEASE don’t open the attachment

- Security considerations? - if you want to replace rich email and attachments with plain text, I’ll support your draft.

Not all Phish Email is Created Equal



From: "American Express" <AmericanExpress@welcome.aexp.com>
Date: Fri, Mar 30, 2012 4:08 pm
Subject: Confirmation of email address change
To: <your email address here>

Thanks for updating your email address

For your security:

Cardmember:

Dear Cardmember,

Thanks for updating your e-mail address with us.

We changed your e-mail address in our files to MelanieGentry@comcast.net. If this is correct, you can disregard this e-mail. If the new e-mail address is not correct or you did not request this change, please click here, or log on to https://www.americanexpress.com/ to change it.

Thank you for your Cardmembership.

Sincerely,
American Express Customer Service

Contact Customer Service | View Our Privacy Statement | Add Us to Your Address Book

Your Cardmember information is included in the upper-right corner to help you recognize this as a **customer service e-mail** from American Express. To learn more about e-mail security or report a suspicious e-mail, please visit us at americanexpress.com/phishing. We kindly ask you not to reply to this e-mail but instead contact us securely via the customer service link above.

Copyright 2012 American Express Company. All rights reserved.

AGNEUWEM0002002

http://www.consumerfraudreporting.org/phishing/AmericanExpressScamEmail.php