CE0973a - Issues in Network Security
13: Future Challenges, Planning

James A Sutherland

Abertay University

Monday, 18th April 2016

ISP Background

- Early dialup: static IP! (Demon)
- Later dynamic, allocate and log at dialin
- Still one IP address per customer
- IPv4: 4 billion address globally, ‘enough for everyone. . . ’

ISP Background

- Early dialup: static IP! (Demon)
- Later dynamic, allocate and log at dialin
- Still one IP address per customer
- IPv4: 4 billion address globally, 'enough for everyone. . .'

ISP Background

- Early dialup: static IP! (Demon)
- Later dynamic, allocate and log at dialin
- Still one IP address per customer
- IPv4: 4 billion address globally, ‘enough for everyone. . . ’

ISP Background

- Early dialup: static IP! (Demon)
- Later dynamic, allocate and log at dialin
- Still one IP address per customer
- IPv4: 4 billion address globally, ‘enough for everyone. . . ’

ISPs now

- More customers than IPv4 addresses
- No IPv6 critical mass (yet)
- So, customers have to share: CGNAT
- Not to mention WiFi

ISPs now

- More customers than IPv4 addresses
- No IPv6 critical mass (yet)
- So, customers have to share: CGNAT
- Not to mention WiFi

ISPs now

- More customers than IPv4 addresses
- No IPv6 critical mass (yet)
- So, customers have to share: CGNAT
- Not to mention WiFi

ISPs now

- More customers than IPv4 addresses
- No IPv6 critical mass (yet)
- So, customers have to share: CGNAT
- Not to mention WiFi

What's in an IP?

- An IPv4 address used to identify a customer
- Not a person, though, important distinction
- With CGNAT, it doesn't even identify that much
- Port mapping logs expand rapidly, need time+IP for ID

What's in an IP?

- An IPv4 address used to identify a customer
- Not a person, though, important distinction
- With CGNAT, it doesn't even identify that much
- Port mapping logs expand rapidly, need time+IP for ID

What's in an IP?

- An IPv4 address used to identify a customer
- Not a person, though, important distinction
- With CGNAT, it doesn't even identify that much
- Port mapping logs expand rapidly, need time+IP for ID

What's in an IP?

- An IPv4 address used to identify a customer
- Not a person, though, important distinction
- With CGNAT, it doesn't even identify that much
- Port mapping logs expand rapidly, need time+IP for ID

Who did what?

- Important distinction in forensics
- People commit crimes
- Devices hold data
- Addresses download content
- HMA v Barry Stewart, Aberdeen 2014

Who did what?

- Important distinction in forensics
- People commit crimes
- Devices hold data
- Addresses download content
- HMA v Barry Stewart, Aberdeen 2014

Who did what?

- Important distinction in forensics
- People commit crimes
- Devices hold data
- Addresses download content
- HMA v Barry Stewart, Aberdeen 2014

Who did what?

- Important distinction in forensics
- People commit crimes
- Devices hold data
- Addresses download content
- HMA v Barry Stewart, Aberdeen 2014

Who did what?

- Important distinction in forensics
- People commit crimes
- Devices hold data
- Addresses download content
- HMA v Barry Stewart, Aberdeen 2014

Logging Problems

- More servers and routers
- More data to log
- More retention and search requirements
- Investigate abuse, billing, law enforcement
- Central logging servers: syslog, databases
- Timestamps need to match! NTP, timezones (UTC)

Logging Problems

- More servers and routers
- More data to log
- More retention and search requirements
- Investigate abuse, billing, law enforcement
- Central logging servers: syslog, databases
- Timestamps need to match! NTP, timezones (UTC)

Logging Problems

- More servers and routers
- More data to log
- More retention and search requirements
- Investigate abuse, billing, law enforcement
- Central logging servers: syslog, databases
- Timestamps need to match! NTP, timezones (UTC)

Logging Problems

- More servers and routers
- More data to log
- More retention and search requirements
- Investigate abuse, billing, law enforcement
- Central logging servers: syslog, databases
- Timestamps need to match! NTP, timezones (UTC)

Logging Problems

- More servers and routers
- More data to log
- More retention and search requirements
- Investigate abuse, billing, law enforcement
- Central logging servers: syslog, databases
- Timestamps need to match! NTP, timezones (UTC)

Logging Problems

- More servers and routers
- More data to log
- More retention and search requirements
- Investigate abuse, billing, law enforcement
- Central logging servers: syslog, databases
- Timestamps need to match! NTP, timezones (UTC)

Central Logging

- Windows Remote Logging since Vista/2008[1]
- Unix: syslog since 1980s, standardised 2001 RFC3164[2]
- Also SNMP, 1988, RFC1065 on[3]

[1] http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Centralized-Auditing-here-FREE.html

[2] https://tools.ietf.org/html/rfc3164

[3] https://tools.ietf.org/html/rfc1065

Central Logging

- Windows Remote Logging since Vista/2008[1]
- Unix: syslog since 1980s, standardised 2001 RFC3164[2]
- Also SNMP, 1988, RFC1065 on[3]

[1] http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Centralized-Auditing-here-FREE.html

[2] https://tools.ietf.org/html/rfc3164

[3] https://tools.ietf.org/html/rfc1065

Central Logging

- Windows Remote Logging since Vista/2008[1]
- Unix: syslog since 1980s, standardised 2001 RFC3164[2]
- Also SNMP, 1988, RFC1065 on[3]

[1] http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Centralized-Auditing-here-FREE.html

[2] https://tools.ietf.org/html/rfc3164

[3] https://tools.ietf.org/html/rfc1065

Fail-safe v fail-secure

- What if logging fails? Lost server, out of space.
- Fail-safe: continue without logs, or discard older ones.
- Fail-secure: shut down instead. Government systems do that. . .
- McKinnon tried to cover his tracks by filling the logs. Whoops.

Fail-safe v fail-secure

- What if logging fails? Lost server, out of space.
- Fail-safe: continue without logs, or discard older ones.
- Fail-secure: shut down instead. Government systems do that. . .
- McKinnon tried to cover his tracks by filling the logs. Whoops.

Fail-safe v fail-secure

- What if logging fails? Lost server, out of space.
- Fail-safe: continue without logs, or discard older ones.
- Fail-secure: shut down instead. Government systems do that. . .
- McKinnon tried to cover his tracks by filling the logs. Whoops.

Fail-safe v fail-secure

- What if logging fails? Lost server, out of space.
- Fail-safe: continue without logs, or discard older ones.
- Fail-secure: shut down instead. Government systems do that. . .
- McKinnon tried to cover his tracks by filling the logs. Whoops.

Investigation

- Have logs been tampered with?
- Difficult on compromised systems
- Some clever crypto tricks, remote witness
- Tripwire, similar IDS

Investigation

- Have logs been tampered with?
- Difficult on compromised systems
- Some clever crypto tricks, remote witness
- Tripwire, similar IDS

Investigation

- Have logs been tampered with?
- Difficult on compromised systems
- Some clever crypto tricks, remote witness
- Tripwire, similar IDS

Investigation

- Have logs been tampered with?
- Difficult on compromised systems
- Some clever crypto tricks, remote witness
- Tripwire, similar IDS

Testifying

- What does a log really say?
- Not *the user* did X, but *their account* did
- Important enough distinction for suspects to walk!

Testifying

- What does a log really say?
- Not *the user* did X, but *their account* did
- Important enough distinction for suspects to walk!

Testifying

- What does a log really say?
- Not *the user* did X, but *their account* did
- Important enough distinction for suspects to walk!

Terminology Recap

Authentication	Who are you?
Authorisation	What can you do?
Signature	Tamper-detection
Encryption	Read-prevention
Replay attack	Stop things being reused

Terminology Recap

Authentication Who are you?

Authorisation What can you do?

Signature Tamper-detection

Encryption Read-prevention

Replay attack Stop things being reused

Terminology Recap

Authentication	Who are you?
Authorisation	What can you do?
Signature	Tamper-detection
Encryption	Read-prevention
Replay attack	Stop things being reused

Terminology Recap

Authentication	Who are you?
Authorisation	What can you do?
Signature	Tamper-detection
Encryption	Read-prevention
Replay attack	Stop things being reused

Terminology Recap

Authentication	Who are you?
Authorisation	What can you do?
Signature	Tamper-detection
Encryption	Read-prevention
Replay attack	Stop things being reused

Authentication

- Biometrics
- Two-factor
- One-time Passwords
- Cryptographic

Authentication

- Biometrics
- Two-factor
- One-time Passwords
- Cryptographic

Authentication

- Biometrics
- Two-factor
- One-time Passwords
- Cryptographic

Authentication

- Biometrics
- Two-factor
- One-time Passwords
- Cryptographic

Week 13 Tasks

- Look at past papers, check you can answer them all!
- Also try enabling two-factor authentication where you can, e.g. Facebook

Week 13 Tasks

- Look at past papers, check you can answer them all!
- Also try enabling two-factor authentication where you can, e.g. Facebook