Security Evaluation of NTP

Matthew Van Gundy <mvangund@cisco.com>

Technical Leader, Cisco Advanced Security Initiatives Group (ASIG)

Linux Collaboration Summit 2016

Who Are We?

Cisco ASIG:

- ~70 Hardware & Software Security Specialists
- Proactively assesses security of Cisco products and services
- Eval Team: Jonathan Gardner, Stephen Gray, Matt Street

Cisco Talos VulnDev:

- Develop and employ automated tooling to discover open-source software vulnerabilities at scale
- Eval Team: Yves Younan, Aleksandar Nikolic

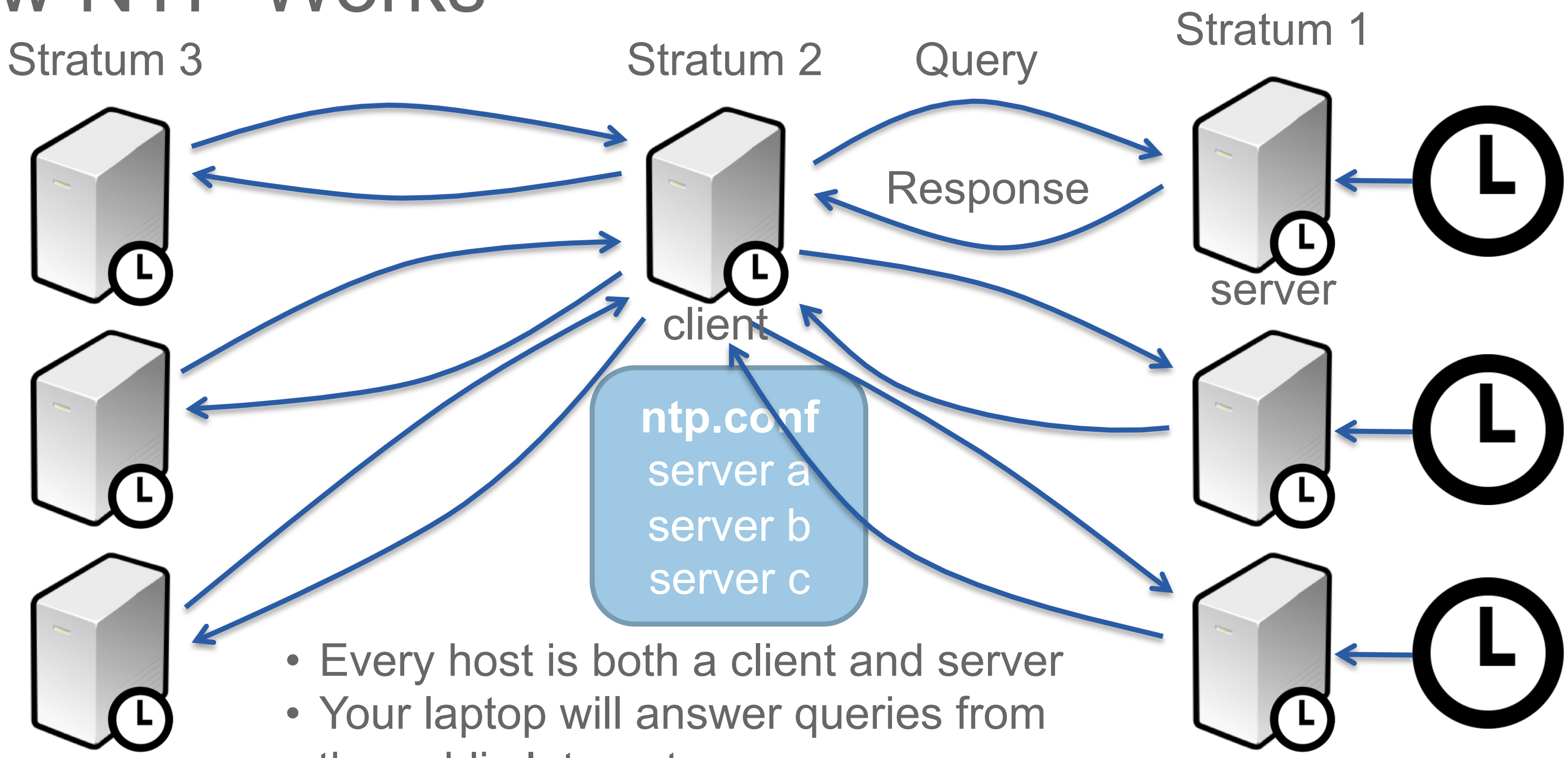
Boston University:

- Aanchal Malhotra, PhD Student
- Sharon Goldberg, Associate Professor

Why Evaluate NTP?

- Accurate time keeping is critical to the safe operation of many Internet systems
- NTP runs *everywhere*: routers, switches, servers, laptops
- All software has flaws
  - A number of serious CVEs disclosed in 2014-2015
  - Previous evaluators stated additional concerns
- In support of Linux Foundation Core Infrastructure Initiative (CII)
- Cisco proactively assesses security of our products and services

How NTP Works



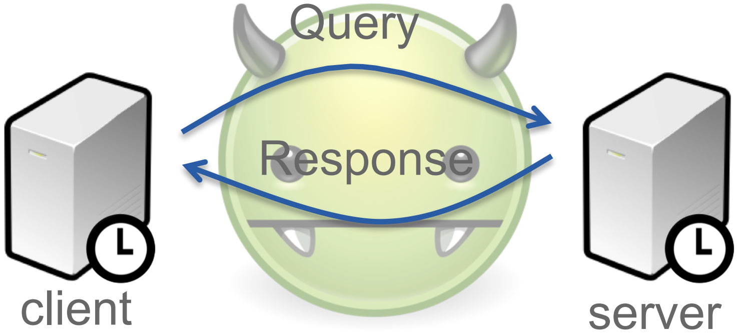
```
ntp.conf
server a
server b
server c
```

- Every host is both a client and server
- Your laptop will answer queries from the public Internet

Image credits: George Boukeas, original Gorilla icon theme artwork by Jakub Steiner (CC BY-SA 3.0), via Wikimedia Commons

Slide Credit: Sharon Goldberg & Aanchal Malhotra

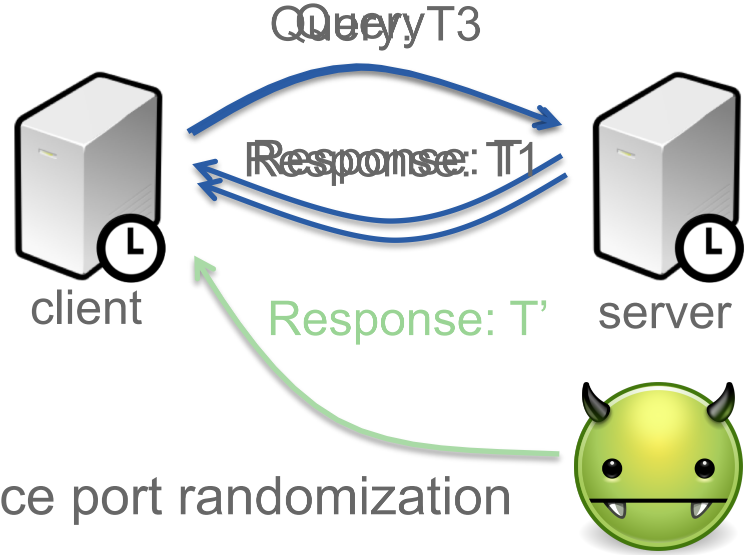
Preventing On-Path Impersonation Attacks



- Crypto prevents on-path attacks
- Rarely used in practice
- Symmetric crypto
  - digest = MD5(key || message)
  - Difficult to manage: manual key distribution
- Asymmetric crypto (Autokey)
  - Autokey Protocol (RFC 5906) is not a standards-track document
  - Autokey is known to be broken (S. Röttger 2012)
  - "… if you are using autokey you should stop using it." -- Harlan Stenn, NTP Maintainer, 2015

Preventing Off-Path Impersonation Attacks

NTP Packet					
LI	Ver	Mode	Stratum (8)	Poll (8)	Precision (8)
Root delay (32)					
Root dispersion (32)					
Reference Clock Id (32)					
Reference Clock Timestamp (64)					
T1: Origin Timestamp (64)					
T2: Receive Timestamp (64)					
T3: Transmit Timestamp (64)					
Keyid (32, optional)					
Digest (128+, optional)					



- No source port randomization
- TEST2: Drop packet unless T3 in query == T1 in response
- Transmit timestamp has ≈ 32-bits entropy
- Similar to TCP sequence number randomization

High-Level Attack Goals

Targets

Program Safety

- ntp 4.2.8p2

Application & Protocol Logic

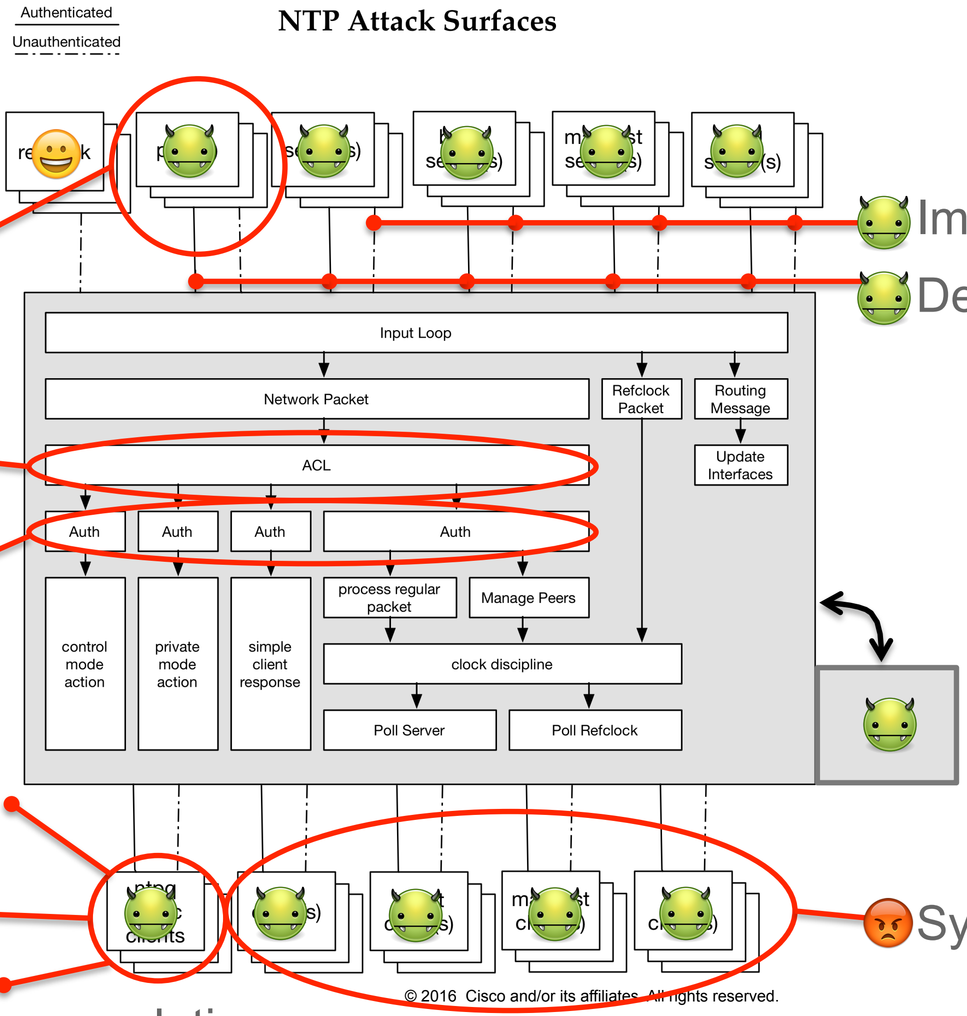
- ntp 4.2.8p3-p6
- NTPsec @{2015-08-19}-0.9.0

Goal	Status
Change Time	😈
Denial of Service	😈
OS-level Privilege Escalation	😈

😈 : Achieved!   😡 : Not Achieved

👿 : Achieved!
😡 : Not Achieved

NTP Attack Surfaces



👿 Add malicious peers

👿 Impersonate servers

👿 Defeat authentication

😡 Bypass ACL

😡 Exploit inconsistency in authentication

👿 Information disclosure

😡 Malicious reconfiguration

😡 Sync with clients

👿 Local privilege escalation

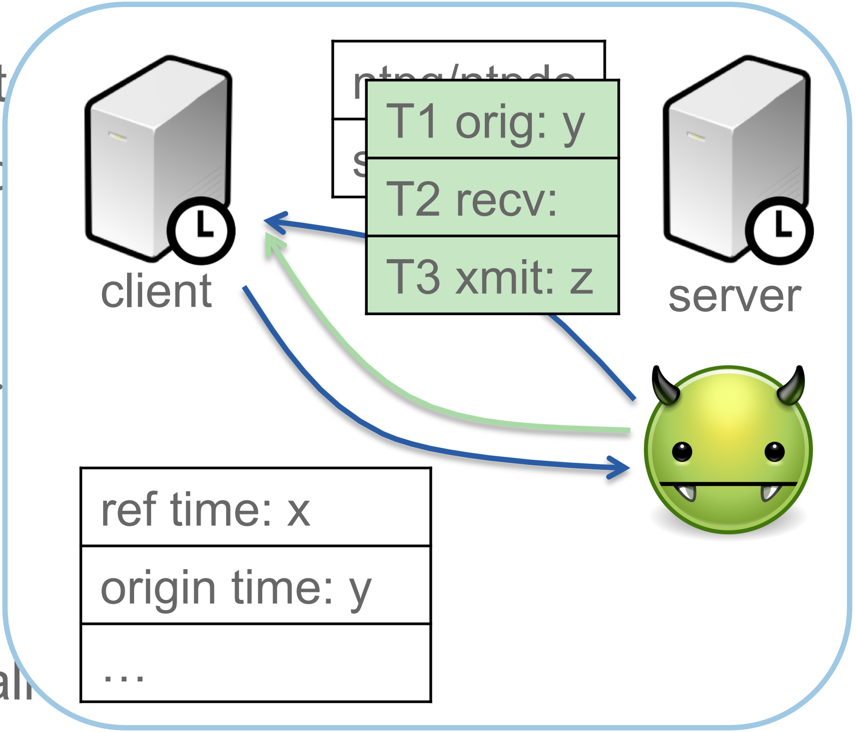
Impersonating Servers - Bypassing Origin Validation

Spoofing Messages from Peers

- Origin timestamp serves as a nonce t
- Control protocols disclose expected c unauthenticated clients (CVE-2015-8

```
ntpdc> showpeer 192.168.33.10
remote 192.168.33.10, local 192.168.33.
...
reference time:      d9c79a0e.1ef70a98
originate timestamp: d9c79a63.b05e631b
receive timestamp:   d9c79a20.b9d5ee3d
transmit timestamp:  d9c79a20.b9d5ee3d
```

- Most systems limit ntpq/ntpdc to locali



client

server

ntpq/ntpdc

s

T1 orig: y

T2 recv:

T3 xmit: z

ref time: x

origin time: y

…

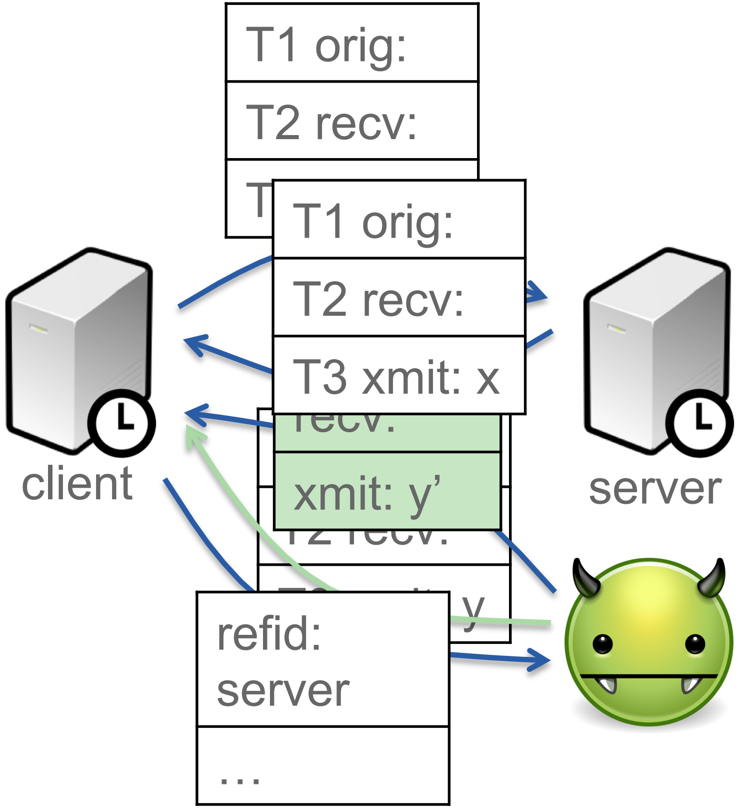
Spoofing Messages from Peers: `0rigin` (CVE-2015-8138)

- RFC 5905 (NTP v4) States:

  To protect against replay of the last transmitted packet, the xmt state variable *is set to zero* immediately after a successful bogus check.

- ntpd advertises time source in reference clock id field

- ntpd accepts more than one message per poll period



Demo:
Changing Time Using Origin (CVE-2015-8138)

Recommendations for Origin Leak
(CVE-2015-8139)

- Improve scrutiny of non-standard extensions
- Prevent access to control protocols

```
ntp.conf:
  disable mode7
  restrict default noquery …
```

- Only allow authorized access

```
iptables -A OUTPUT -o lo -p udp -m udp --dport 123 \
   -m owner --uid-owner root -j ACCEPT
iptables -A OUTPUT -o lo -p udp -m udp --dport 123 \
   -j DROP
```

Recommendations for `0rigin` (CVE-2015-8138)

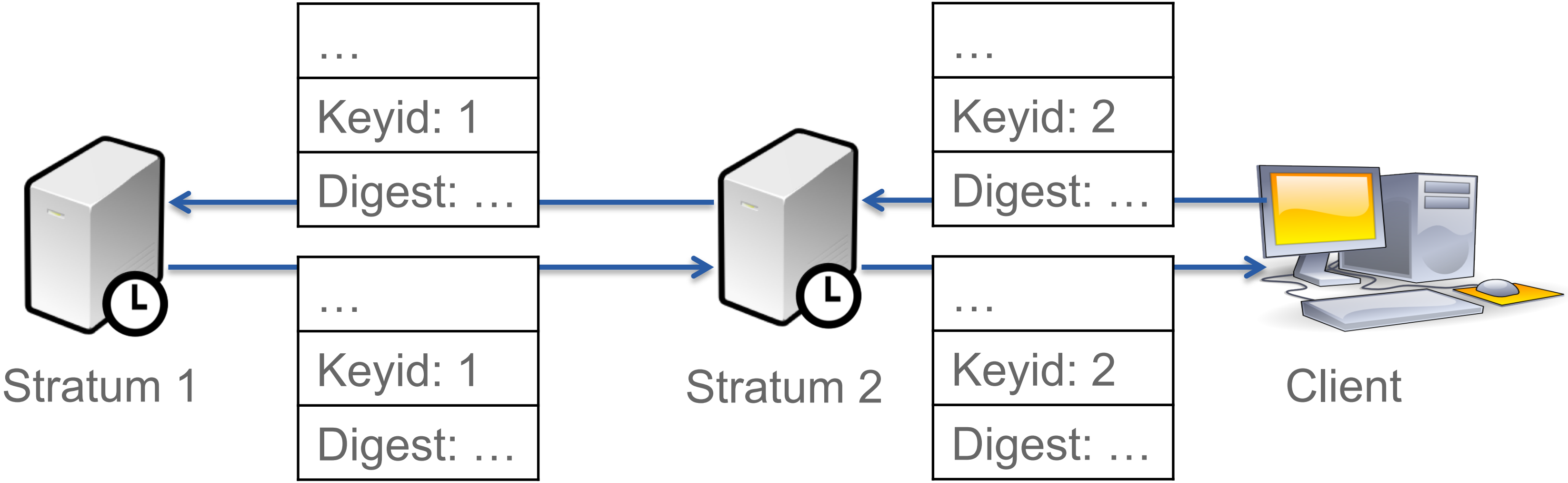
- Improved peer review?
- Limit number of messages accepted per poll period*
- Improved modularity and automated testing
- Clients: Block incoming packets except from configured peers
  - ntp.conf: `restrict default noserve ...`
  - Host-based firewall
- Enable and enforce authentication (if feasible)

```
restrict default notrust ...
trustedkey 1
enable auth
server ntp.localdomain key 1
```

* does not prevent attack

Defeating Authentication

A Typical Authenticated NTP Environment



…

Keyid: 1

Digest: …

…

Keyid: 1

Digest: …

…

Keyid: 2

Digest: …

…

Keyid: 2

Digest: …

Stratum 1

Stratum 2

Client

server stratum1 key 1

server stratum2 key 2

Keys:
1: secret
2:

Keys:
1: secret
2: othersecret

Keys:
1:
2: othersecret

Symmetric Authentication

- digest = MD5(key || message)
- Vulnerable to length extension

  (Only affects autokey and proprietary extensions)
- Difficult to manage
- Standards do not define semantics
- Reject packet if

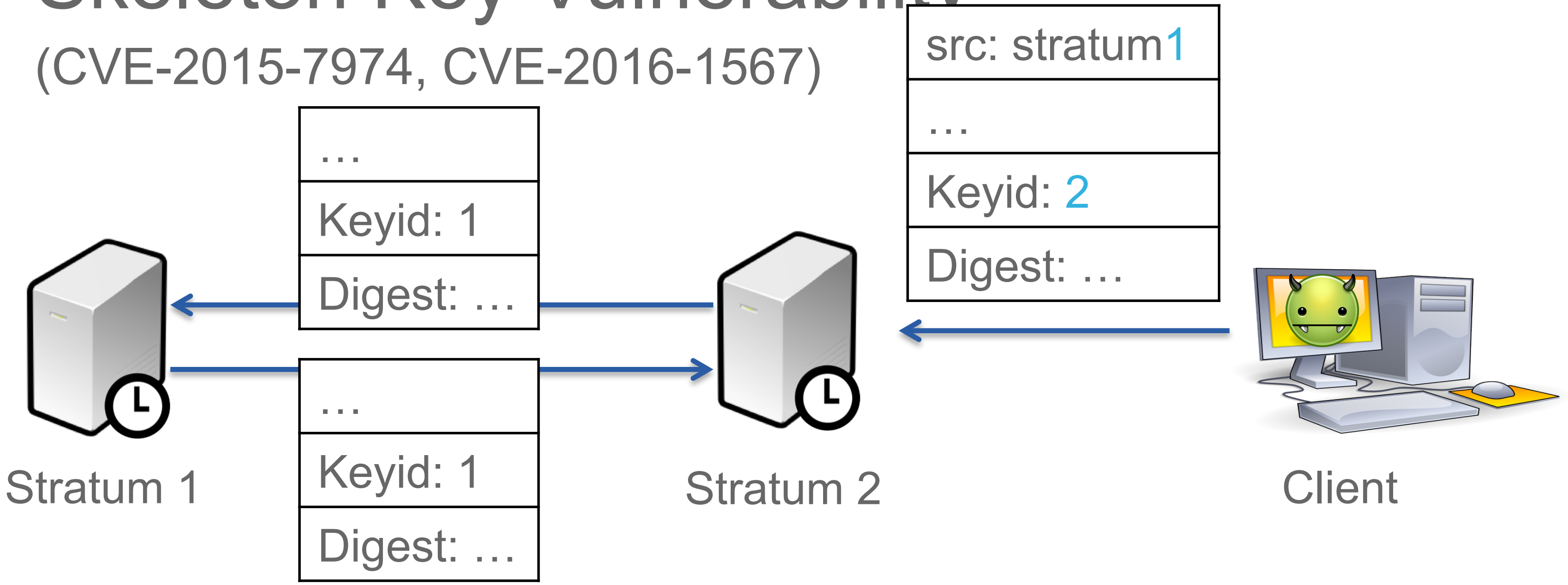
```
MD5(keys[pkt.keyid ] ||
     pkt.msg) != pkt.digest
```

NTP Packet

LI	Ver	Mode	Stratum (8)	Poll (8)	Precision (8)
Root delay (32)					
Root dispersion (32)					
Reference Clock Id (32)					
Reference Clock Timestamp (64)					
T1: Origin Timestamp (64)					
T2: Receive Timestamp (64)					
T3: Transmit Timestamp (64)					
Keyid (32, optional)					
Digest (128+, optional)					

Skeleton Key Vulnerability

(CVE-2015-7974, CVE-2016-1567)



…
Keyid: 1
Digest: …

…
Keyid: 1
Digest: …

src: stratum1
…
Keyid: 2
Digest: …

Stratum 1

Stratum 2

Client

Keys:
1: secret
2:

server stratum1 key 1

Keys:
1: secret
2: othersecret

server stratum2 key 2

Keys:
1:
2: othersecret

Recommendations for Skeleton Key
(CVE-2015-7974, CVE-2016-1567)

- Improved peer review?
- Standardize clear and precise definition of NTP authentication
- Upgrade to ntp 4.2.8p6 or above

Adding Malicious Peers - Ephemeral Associations

Ephemeral Associations

- RFC 5905 (NTP v4) :

  Ephemeral associations are mobilized upon the arrival of a packet and are demobilized upon error or timeout

- Supported for symmetric, broadcast, and manycast modes
- Packets mobilizing new ephemeral associations must be authenticated (by default)

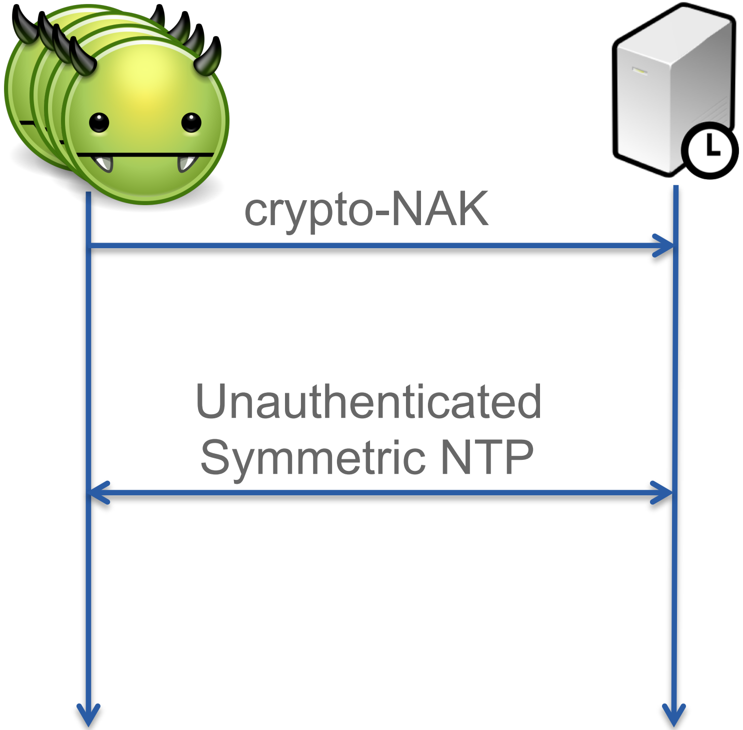
Crypto-NAK Packets

- Authentication errors elicit a crypto-NAK response
- Not authenticated
- crypto-NAK packets are handled “late”, during other packet consistency checks
- Authentication states:
  { NONE, OK, ERROR, CRYPTO }

<table>
<tr><th colspan="6">NTP Crypto-NAK Packet</th></tr>
<tr><td>LI</td><td>Ver</td><td>Mode</td><td>Stratum (8)</td><td>Poll (8)</td><td>Precision (8)</td></tr>
<tr><td colspan="6">Root delay (32)</td></tr>
<tr><td colspan="6">Root dispersion (32)</td></tr>
<tr><td colspan="6">Reference Clock Id (32)</td></tr>
<tr><td colspan="6">Reference Clock Timestamp (64)</td></tr>
<tr><td colspan="6">T1: Origin Timestamp (64)</td></tr>
<tr><td colspan="6">T2: Receive Timestamp (64)</td></tr>
<tr><td colspan="6">T3: Transmit Timestamp (64)</td></tr>
<tr><td colspan="6"><i>Keyid (32, optional) == 0x00000000</i></td></tr>
<tr><td colspan="6"><s><i>Digest (128+, optional)</i></s></td></tr>
</table>

NAK to the Future Vulnerability (CVE-2015-7871)

- Most ephemeral associations
  - auth in {ERROR, CRYPTO}: reject
  - auth == NONE: reject if auth required
  - else: mobilize
- Symmetric active mode packets
  - auth in {NONE, ERROR}: Special handling for certain broken clients
  - else: mobilize
  - (auth == CRYPTO): crypto-NAK packets mobilize new symmetric associations
- keyid == 0: Unauthenticated association



Peers:

- server
- attacker

Recommendations for NAK to the Future
(CVE-2015-7871)

- Introduced through refactoring in 4.2.5p186
- Use language / compiler features

  `enums and switch + gcc -Wswitch`
- Clients: Block incoming packets except from configured peers
- Block crypto-NAK packets using deep packet inspection
- Drop NTP packets unless the level 3 payload length is one of
  - 48 bytes (unauthenticated)
  - 68 bytes (symmetric MD5)
  - 72 bytes (symmetric SHA1)

When NTP panics

PANIC: Preventing large time shifts

- RFC 5905 (NTP v4) :

  PANIC means the offset is greater than the panic threshold PANICT (1000 s) and SHOULD cause the program to exit with a diagnostic message to the system log.

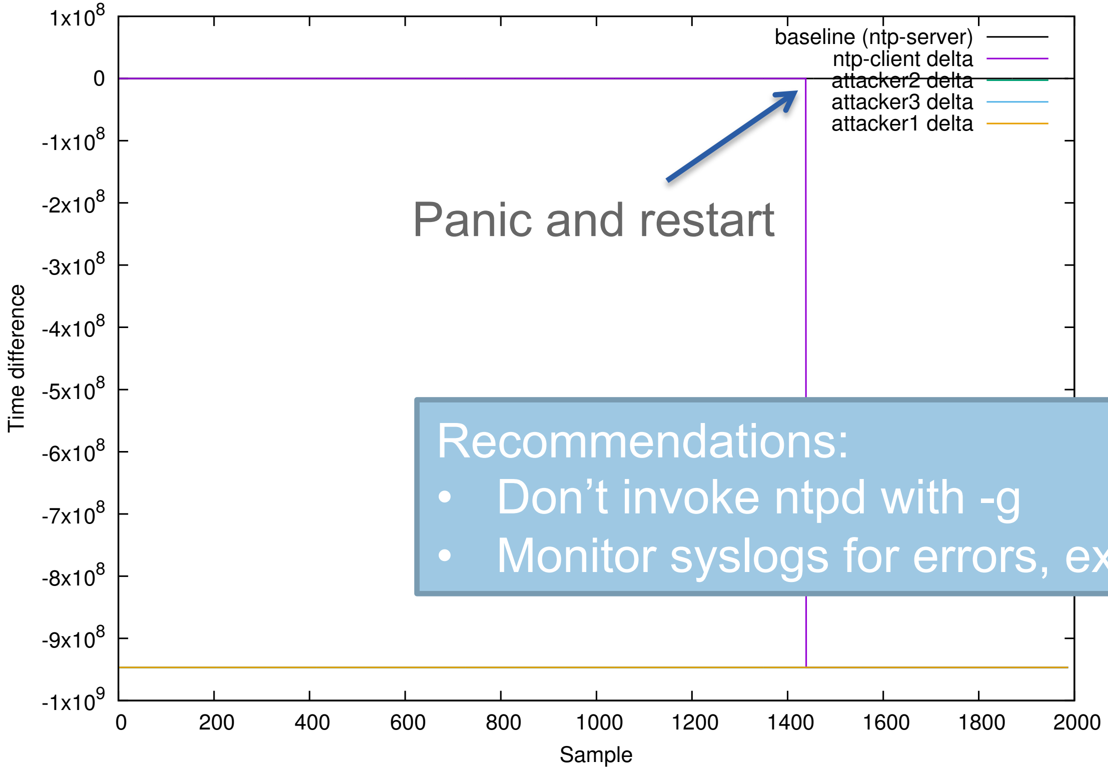
- Many systems invoke ntpd with the -g flag

  This option allows the time to be set to any value without restriction; however, this can happen only once.

- Process supervisors restart failed daemons

- Sometimes ntpd will STEP more than once (Malhotra et al. CVE-2015-5300)

Going Back to 1985



Panic and restart

Recommendations:

- Don’t invoke ntpd with -g
- Monitor syslogs for errors, exits, and restarts

Other Vulnerabilities

Other Vulnerabilities

- Déjà vu: Broadcast traffic can be replayed by on-path attackers (CVE-2015-7973)[1]
- Unauthenticated off-path DoS against preemptable modes (CVE-2015-7979)[1]
- Buffer overflow via refclock (CVE-2015-7853)

[1] Malhotra & Goldberg. "Attacking NTP's Authenticated Broadcast Mode." ACM SIGCOMM Computer Communication Review, April 2016.

Server-side (ntpd) Control Mode Vulnerabilities

Unauthenticated

- Control messages can be replayed (CVE-2015-8140)
- DoS via ntpq reslist command (CVE-2015-7977, CVE-2015-7978)

Authenticated

- 1 use-after free (CVE-2015-7849)
- 2 denial-of-service (CVE-2015-7848, CVE-2015-7850)
- 1 directory traversal on VMS (CVE-2015-7851)
- 1 creation of file with unsafe path (CVE-2015-7976)

Client-side (ntpq/ntpdc) Control Mode Vulnerabilities

Unauthenticated

- 1 server-exploitable infinite loop DoS (CVE-2015-8158)

Authenticated

- 2 local buffer overflows (CVE-2015-7854, CVE-2015-7975)
- 1 off-by-one memory corruption (CVE-2015-7852)

Recommendations:

- Limit access to control protocols

Vulnerability Summary

Impact	Unauthenticated	Authenticated	Total
Time-Shifting	5	1	6
Server Escalation	0	4	4
Client Escalation	1	1	2
Server DoS	2	2	4
Client DoS	3	0	3
To Be Disclosed			5
Total	11	8	24

NTP / NTPsec Wins

- Interleaved Modes
- Pool Mode
- Manycast Mode
- Orphan Mode
- Dynamic Server Discovery

- IP-based Access Control
- Clock Selection
- Leap Second Handling
- NTPsec Modifications

Areas for Future Investigation

- Network Time Security (draft replacement for Autokey)
- Attacking reference clocks
  - Spoofing upstream time sources
  - Exploiting refclock drivers
- IP ACL consistency
- Clock selection
- ntpq traps

How You Can Help

- Conduct security evaluations
- Contribute developer resources to NTP and NTPsec
  - Modularization
  - Testing
- Contribute tooling and other infrastructure

CISCO TOMORROW starts here.

http://www.talosintel.com/vulnerability-reports/

Demo:
Changing Time Using NAK to the Future

NTP Control Protocols (ntpq, ntpdc)

- Two control protocols: ntpq (mode 6), ntpdc (mode 7, deprecated)
- Read ntpd parameters: variables, counters, peer list, peer attributes
- Write many ntpd parameters
  - Dynamic reconfiguration
  - Requires authentication
- Previously used in large-scale DDoS attacks
- Restricted to localhost by default on many modern systems

Hardening your NTP daemons

- Keep up on security patches
- Use safe default restrictions

  ```
  restrict default notrap
  nomodify nopeer
  ```
- Disable ntpdc entirely
- Restrict access to control protocols as much as possible
- Use firewall to limit local access to control protocols to authorized users
- Use firewall to restrict NTP traffic to configured peers
  - Clients: block inbound NTP packets that are not part of an established session
  - Servers: block inbound symmetric and server NTP packets that are not part of an established session

Hardening your NTP daemons

- Enable authentication if possible
- Disable unauthenticated traffic by default
- Whitelist known-good unauthenticated peers
- Use firewall rules to drop crypto-NAK packets
- Disable unpeering on error

- Remove unused ntp.conf trustedkeys
- Do not invoke ntpd with -g
- Run ntpd as an unprivileged user
- Confine ntpd using Mandatory Access Controls
- Consider chroot jailing ntpd