Demonstrating Covert Channel Vulnerabilities in Precision Time Protocol (PTP)

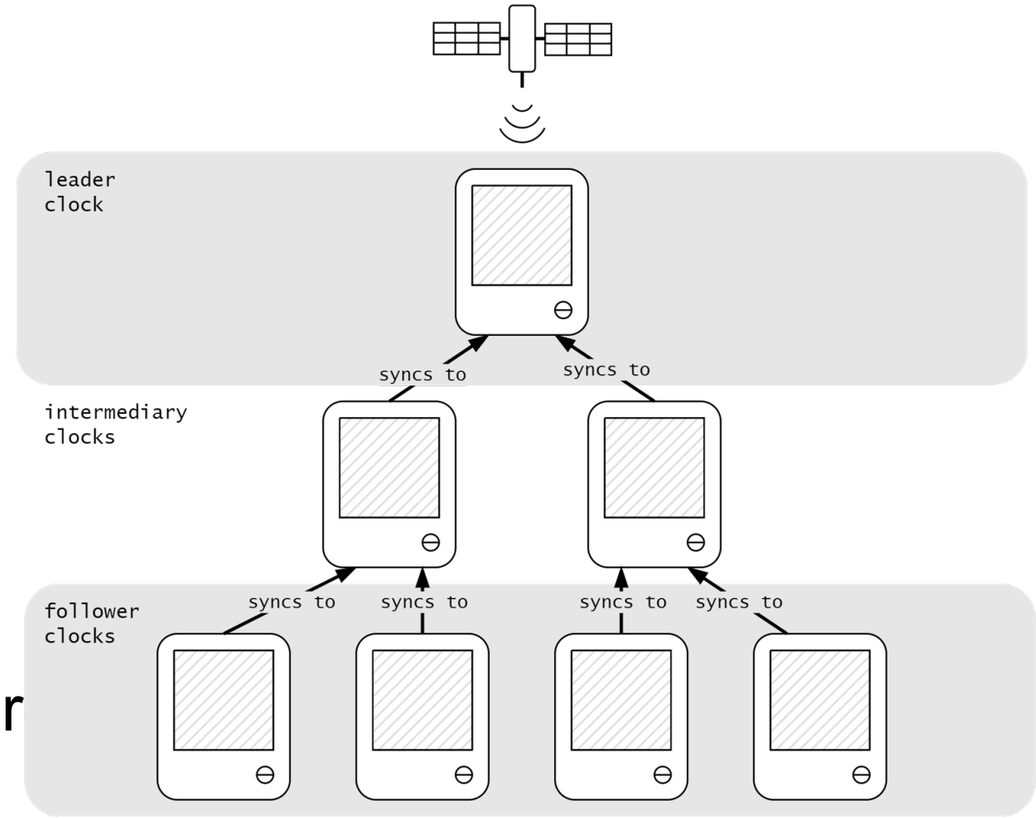
March 14th, 2023

Aron Smith-Donovan, Abby Marsh
Macalester College

WSTS 2023
Vancouver, BC

Overview — Precision Time Protocol (PTP)

- IEEE 1588 standard
  - first defined in 2002 as alternative to Network Time Protocol (NTP)
- highly accurate clock synchronization within local networks
  - majority of devices lack necessary hardwar for satellite or Internet connectivity and cannot access external time sources



Overview — Covert Channels

- communicate information outside of normal channels
  - use methods not anticipated in normal operation
  - not covered by standard security policies
  - often difficult to detect
- hiding information where someone wouldn't think to check
  - in networks: hiding a secret message inside a non-secret message
- how can we evaluate potential covert channels?
  - **throughput** = amount of data that can be transmitted
  - **detectability** = ability to resist both general and targeted detection measures
  - **robustness**= ability to maintain communication despite potential disruptions

Covert Channel Approaches

- classifying covert channels:
  - encoding approach used
  - type of data object affected
  - potential usage contexts
- potential targets:
  - unvalidated fields
  - optional fields
  - configurable structures
  - configurable intervals
  - on-demand messages

direct = writing data directly

indirect = affecting behaviors or configurations

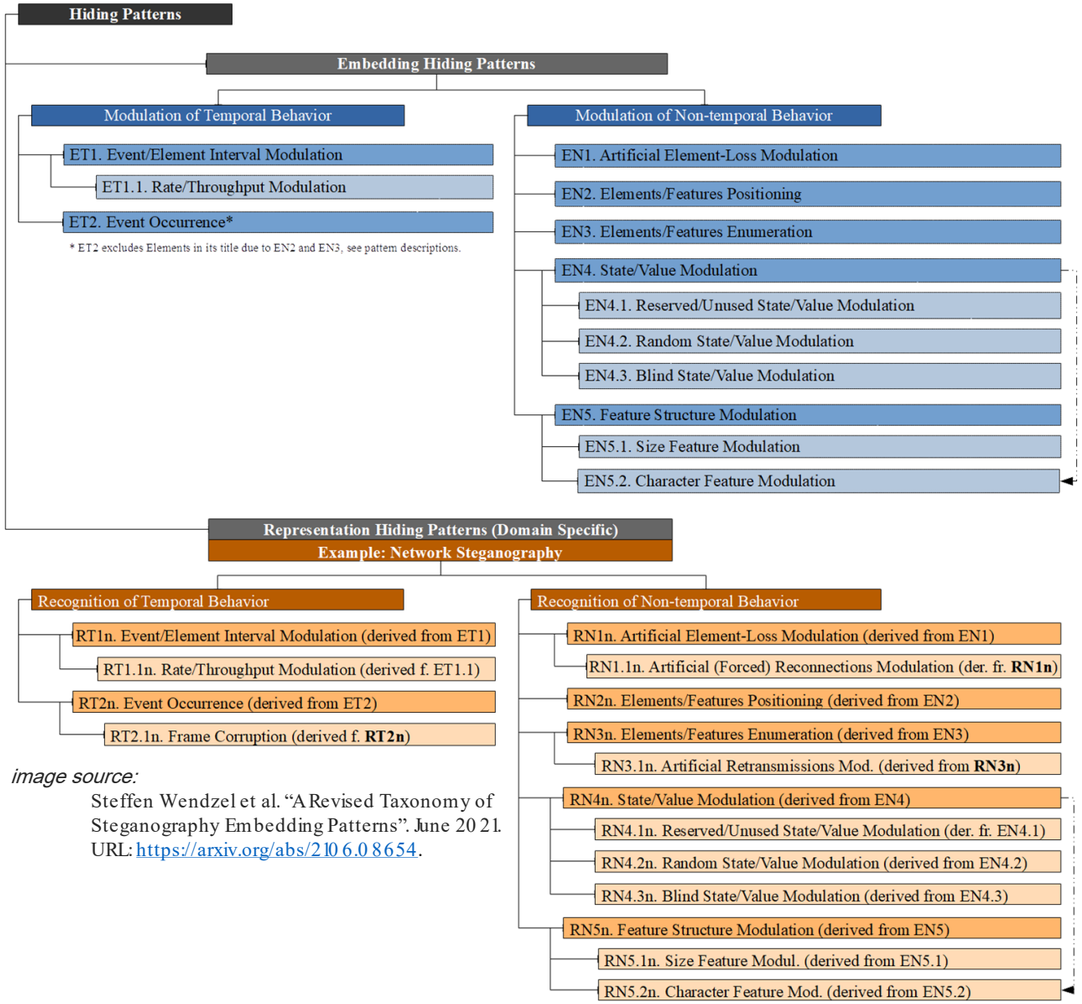


image source:
Steffen Wendzel et al. "A Revised Taxonomy of Steganography Embedding Patterns". June 2021. URL: https://arxiv.org/abs/2106.08654.

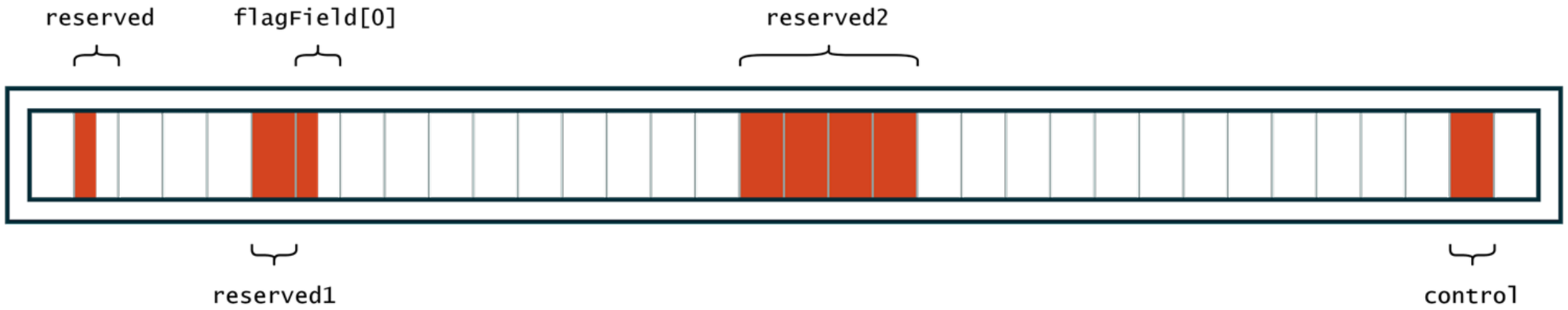
PTP Vulnerability Assessment

- determining potential covert channels:
  - which approaches are impossible?
  - which approaches impede functionality?
- assessing potential strategies
  - throughput, detectability, robustness
- feasible options:
  - **forced reconnections modulation**
  - **artificial retransmissions modulation**
  - **unused value modulation**

Pattern name	Evaluation	Reason
Event/Element Interval Modulation	possible, but not feasible	likely to impair function and/or throw errors → high detectability
Rate/Throughput Modulation	possible, but not feasible	likely to impair function and/or throw errors → high detectability
Event Occurrence	not possible	no suitable target objects
Frame Corruption	possible, but not feasible	viable throughput conditions likely to impair function and/or throw errors → high detectability
Artificial Element-Loss	possible, but not feasible	likely to impair function and/or throw errors → high detectability
Artificial (Forced) Reconnections Modulation	feasible	not likely to throw errors; throughput limited by network configuration; false-positive rate high
Elements/Features Positioning	not possible	no suitable target objects
Elements/Features Enumeration	not possible	no suitable target objects
Artificial Retransmissions Modulation	feasible	not likely to throw errors; increased throughput conditions also increase detectability
State/Value Modulation	possible, but not feasible	likely to impair function and/or throw errors → high detectability
Reserved/Unused State/Value Modulation	feasible	not likely to throw errors; throughput limited by established message rates; false-positive rate low
Random State/Value Modulation	not possible	no suitable target objects
Blind State/Value Modulation	possible, but not feasible	likely to impair function and/or throw errors → high detectability
Feature Structure Modulation	possible, but not feasible	likely to impair function and/or throw errors → high detectability
Size Feature Modulation	possible, but not feasible	likely to impair function and/or throw errors → high detectability
Character Feature Modulation	not possible	no suitable target objects

Covert Channel Development

- selected approach: **unused value modulation**
- PTP message header
  - metadata structure included in all PTP message types
  - 34 bytes long, 7 bytes unused



Covert Channel Prototype — Text Encoding

1 text file:

string:

```
"payload"
```

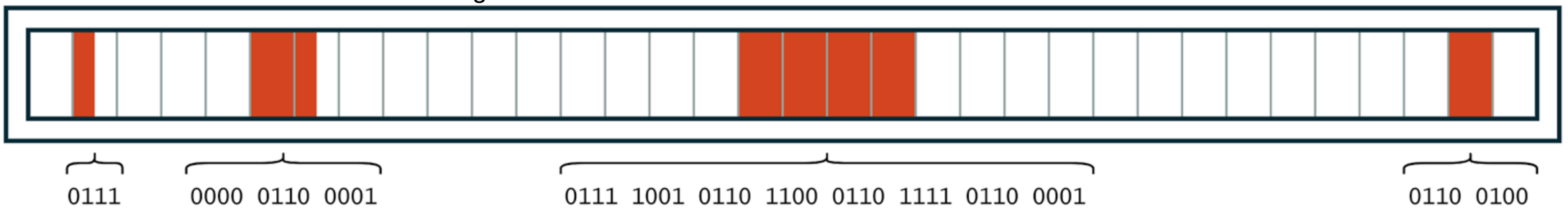
2 array of hexadecimal ASCII encodings:

```
{0x70, 0x61, 0x79, 0x6C,
 0x6F, 0x61, 0x64}
```

3 array of binary values:

```
{0111, 0000, 0110, 0001,
0111, 1001, 0110, 1100, 0110,
1111, 0110, 0001, 0110, 0100}
```

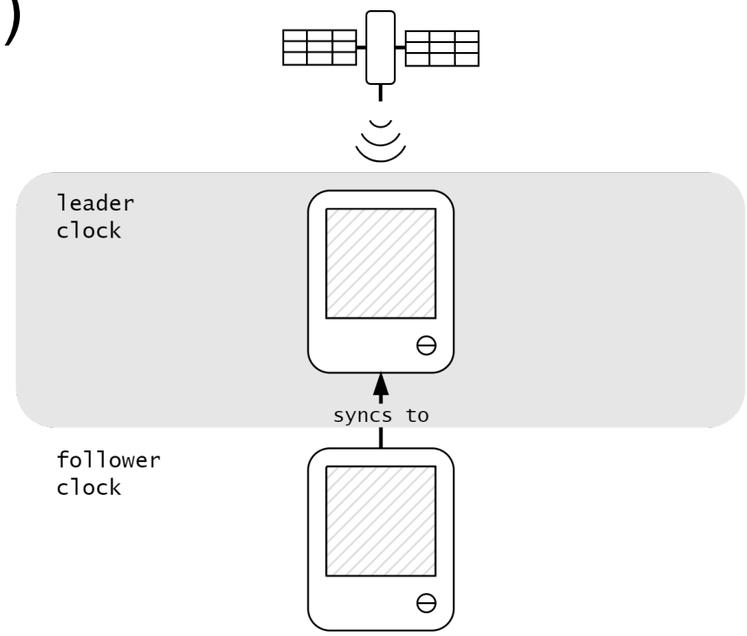
4 encoded in unused values of PTP message header:



Covert Channel Assessment

- detectability
  - no observed change in message rates (±0.01 seconds)
  - no explicit errors
- throughput
  - overall: 7 bytes/message
  - leader ⇨ follower: 24.36 bytes/second
  - follower ⇨ leader: 6.95 bytes/second

Metric	Value		
	Encoded leader	Encoded follower	Encoded overall
time connected	607.52 seconds	600.81 seconds	607.52 seconds
total transmitted	2115 messages	597 messages	2712 messages
transmission rate	3.48 messages/second	0.99 messages/second	4.46 messages/second
channel throughput	24.36 bytes/second	6.95 bytes/second	24.36 bytes/second



Risk Assessment

- covert channel limitations:
  - require high level of access, more likely to appear as tools in a larger attack
  - implementation is difficult and requires extensive knowledge of the target, malicious actors likely to use easier approaches when possible
- standalone attack scenarios:
  - data exfiltration
  - data insertion
- compound attack scenarios:
  - communication channel
  - reconnaissance

Remediation and Prevention

- covert channel remediation:
  - demonstrated approach (unused value modulation) can be prevented with field validation techniques
  - covert channel detection and prevention measures are highly targeted and can only be established after a vulnerability is discovered
- general prevention:
  - implement thorough validation and error checking
  - assess for vulnerabilities and prioritize security at all stages
  - consider potential attack consequences for specific environments
    - critical use cases, including industrial control systems (ICSs), should anticipate extensive damage in the event of a successful attack

Summary and Conclusion

- covert channels
  - targeted remediation is possible for known vulnerabilities
  - general security best practices can restrict utility by decreasing throughput or increasing detectability
- PTP
  - vulnerable to covert channel-based attacks; recent research has demonstrated additional vulnerabilities not covered here
  - standalone attack unlikely due to difficulty of access
- asking the right questions:
  - how might this environment be vulnerable to cyberattacks?
  - what damage could we expect if a successful attack occurred?
  - how can we prevent this attack and/or reduce the potential damage?

Thank you!

Aron Smith-Donovan, *Macalester College*
aronsmithdonovan@gmail.com

Dr. Abby Marsh, *Macalester College*
amarsh1@macalester.edu

Read the full paper:

tinyurl.com/PTPcovertASmithDonovan