Can Digital Evidence Endure the Test of Time?

By

Michael Duren, Chet Hosmer

Presented At

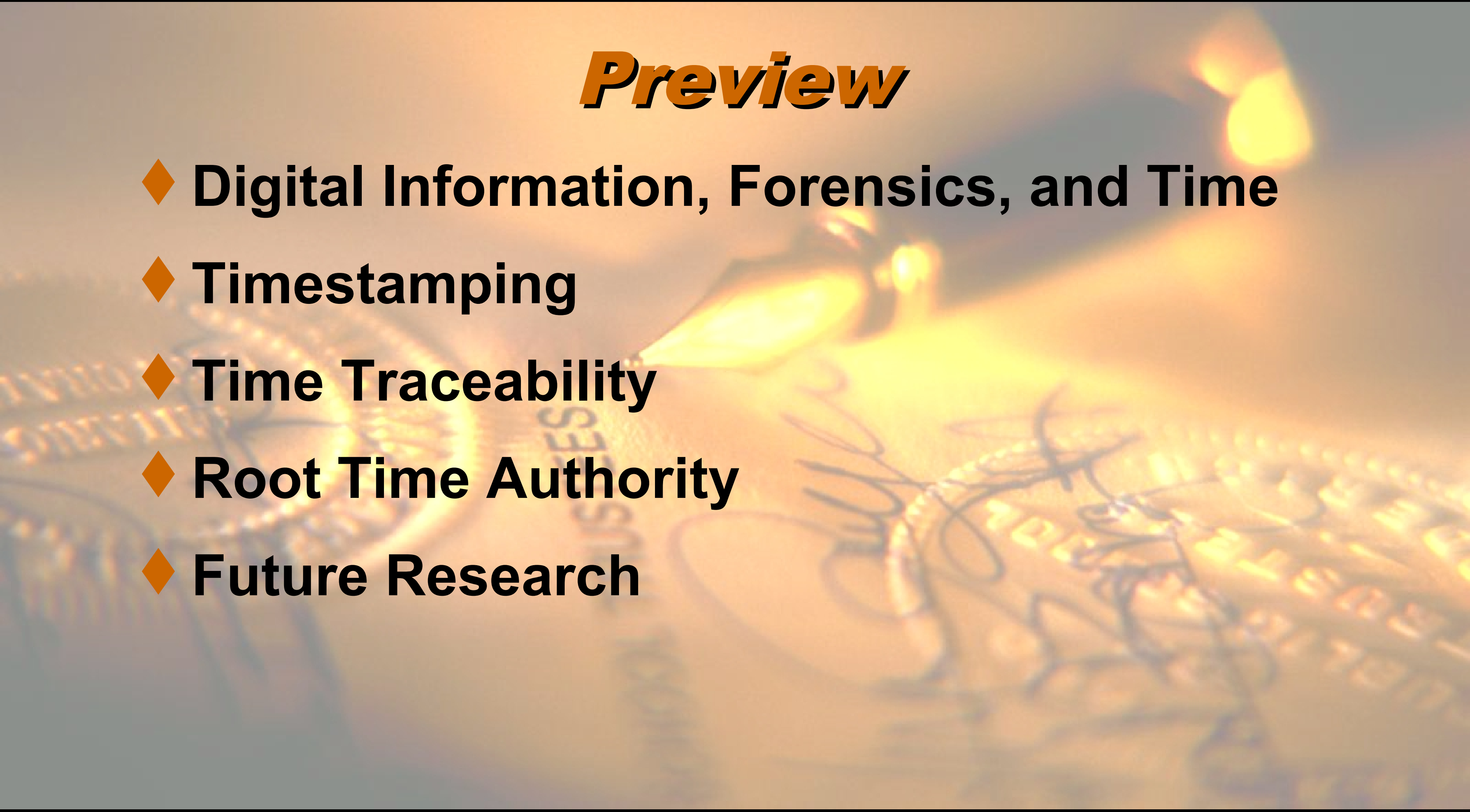
The Digital Forensic Research Conference

DFRWS 2002 USA Syracuse, NY (Aug 6th - 9th)

Can Digital Evidence Endure the Test of Time?

Digital Forensics Research Workshop (DFRWS)
August 7, 2002
Michael Duren
WetStone Technologies, Inc.

Can Digital Evidence Endure the Test of Time?



Preview

- Digital Information, Forensics, and Time
- Timestamping
- Time Traceability
- Root Time Authority
- Future Research

Digital Information

- Amount of digital information generated on a daily basis is unfathomable
- The impact on forensics is profound
- Likelihood that a case involves digital information is very high
  - Phone records, email, transaction logs, accounting data, etc.
- Digital data integrity must be maintained for effective analysis and possible presentation in court

Can Digital Evidence Endure the Test of Time?

Integrity

Integrity can be defined as:

"the property whereby digital data has not been altered in an unauthorized manner since the time it was created, transmitted, or stored by an authorized source". [1]

What about the "When"?

- Cryptographic algorithms can be used to ensure that data has not been altered
  - Digital hashes such as SHA-1 and SHA-2 ensure "content integrity"
  - Asymmetric cryptography and Digital Signing ensure "identity integrity"
- We know how to protect the "who" and the "what"
- What about the "when"?

Can Digital Evidence Endure the Test of Time?

What time was it?

- Time Questions:
  - When was the data created?
  - When was the data modified?
  - When was data collected as evidence?
  - How long did the collection process take?
  - When was the data catalogued?
  - When was it analyzed?
- These questions may seem easy to answer, but how do you prove the answers?

Time Integrity

- Time has been largely overlooked in integrity solutions
- Time is often assumed to be accurate and trusted
  - Amazing to consider everyone’s watch is synchronized within a few minutes
  - You probably know if your watch is a few minutes fast or a few minutes slow
- System clocks are not accurate and are very easily modified

Timestamping

- Computer security experts have recognized the importance of time in security systems
- Public Key Infrastructure (PKIX) working group of the Internet Engineering Task Force (IETF) recognized this as an issue
  - Public Key Cryptosystems require trustworthy time for expiration of certificates and CRL’s
  - Published RFC-3161, “Internet X.509 Public Key Infrastructure Time-Stamp Protocol”

Can Digital Evidence Endure the Test of Time?

Timestamping

- RFC-3161 binds time and digital content using digital signatures
- Timestamps are issued by a Time Stamp Authority (TSA)
- Specification requires the relying party to trust the TSA through the application of policy
- There is no defined mechanism to convey traceability of timestamp’s time

Can Digital Evidence Endure the Test of Time?

Timestamping

RFC 3161 Timestamp:

UTC Time:
August 1, 2002 21:26:46 UTC

Message
Imprint

```
30 82 02 85 06 09       48 86 f7 0d 01 07 02 a0 82 02 76    82 02 72 02 01 03 31 0b 30 09 06 05
2b 0e 03 02 1a 05    30 81 e9 06 0b 2a 86 48 86 f7 0d 01 09 10 01 04 a0 81 d9 04 81 d6 30 81 d3
02 01 01 06 0a 2b 06 01 04 01 84 59 0a 03 01 30 21 30 09 06 05 2b 0e 03 02 1a 05 00 04 14 b7 b8
eb ba 1c 96 76 e  bf 32 e3 e8 18 18 e2 1c c0 93 9c 90 02 04 00 06 38 01 18 13 32 30 30 32 30 38
30 31 32 31 32 36 34 36 2e 38 30 34 5a 30 0a 02 01 00 80 02 01 f4 81 01 00 01 01 ff 02 08 dc a9
a0 eb c8 2e ce ef a0 6b a4 69 30 67 31 0b 30 09 06 03 55 04 06 13 02 55 53 31 11 30 0f 06 03 55
04 0a 13 08 57 65 74 53 74 6f 6e 65 31 33 30 31 06 03 55 04 0b 13 2a 44 61 74 75 6d 20 54 72 75
73 74 65 64 20 54 69 6d 65 20 53 74 61 6d 70 53 65 72 76 65 72 20 53 4e 3a 39 30 44 30 30 32 34
38 31 10 30 0e 06 03 55 04 03 13 07 50 61 75 6c 33 31 39 31 82 01 72 30 82 01 6e 02 01 01 30 47
30 42 31 0b 30 09 06 03 55 04 06 13 02 55 53 31    30 0c 06 03 55 04 0a 13 05 44 61 74 75 6d 31
13 30 11 06 03 55 04 0b 13 0a 46 61 63 74 6f 72 79       41 31 0e 30 0c 06 03 55 04 03 13 05 44
61 74 75 6d 02 01 02 30 09 06 05 2b 0e 03 02 1a 05          30 1a 06 09 2a 86 48 86 f7 0d 01
09 03 31 0d 06 0b 2a 86 48 86 f7 0d 01 09 10 01                                        04 31 16
04 14 ae 88 f1 e5 65 f8 1c 06 b0 ab 54 da ba                                           86 f7
0d                         30 7f 30 7d 30 63                                           97 5c
9f                         a4 44 30 42 31 0b                                           06 03
55                         6d 31 13 30 11 06 03                                     43 41 31
0e 30 0c 06 03 55 04 03 13    44 61 74 75 6d 02 01 02 30 16 04 14 ac 61 74 39 00 4f 9b 1b 4f af
33 97 4e d6 ba 3e 5f 6a 1d 1e 30 0b 06 07 2a 86 48 ce 38 04 03 05 00 04 30 30 2e 02 15 00 a9 1e
dc e4 a9 1d 74 05 7f 02 fb b6 a1 4f fd 13 e0 5d 98 c3 02 15 00 b9 b0 63 4b 32 fb 60 3c 65 b7 1a
37 29 90 27 71 85 73 a7 dc
```

TSA Name:
C=U;O=WetStone;OU=Datum Trusted Time
StampServer SN:90D00248;CN=Paul319

Digital Signature

WetStone
Securing Digital Integrity

Timestamp Traceability

- Timestamps must be traceable!
- Traceability can be defined as:
  - *The property of a result of a measurement or the value of a standard whereby it can be related to stated references, usually national or international standards, through an unbroken chain of comparisons all having stated uncertainties. [4]*
- How can we demonstrate traceability of a timestamp?
- We must define:
  - Our national or international standard
  - An unbroken chain of comparisons

Time Reference

- Many calendars have been created and used over the centuries
- Early calendars where based on the moon
- The calendar used today is the Gregorian calendar and was created in 1582 by Pope Gregory XIII
- The second was defined in 1967 based on measuring the decay of the Cesium atom
- In 1972, the Treaty of the Meter was expanded to include Coordinated Universal Time (UTC) which replaced Greenwitch Mean Time (GMT)

Time Reference

- More than 40 countries contribute to UTC
- UTC is not maintained in a single location; it is virtual
- Contributors compare their clocks and then make appropriate adjustments
- UTC is coordinated in Paris by the International Bureau of Weights and Measures (BIPM)
- The US has two UTC contributors: NIST and USNO

Timestamping Solution

- WetStone has been working on this problem for more than four years
- Combined work with ARFL and our commercial partner Datum, Inc.
  - Phase I and II SBIR, Trusted Network Time
- Solution provides traceability of timestamps to UTC

Timestamping Solution

- TSAs cannot always be located remotely
  - Particularly in transaction based systems
- Assume a requirement for timestamps to be issued on site
- Considering the deployment environment, a basic principal of on-site timestamping device:
  - The Clock and the Cryptographics used in the timestamp must reside in the same cryptographic boundary.
- Problem reduced to showing the traceability of the clock

Timestamping Solution

- Secure Time Module (STM) was developed on the IBM 4758
  - Device is certified at FIPS 140-1 level 4
- Clock and the Crypto reside in the security boundary
- Software in the device follows strict rules for key usage and clock management

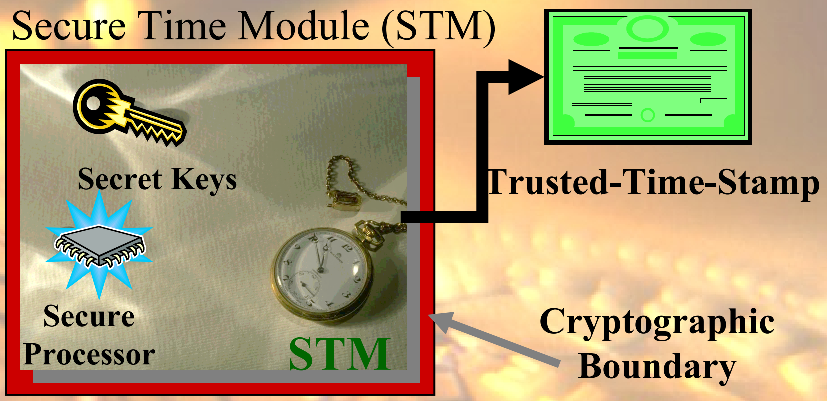


Figure 2. The Secure Time Module

Timestamping Solution

- Traceability can be accomplished through audit
- Defined a Trusted Third Party (TTP) called a Root Time Authority (RTA) that facilitates audits of STM clocks
- On a periodic basis, RTA measures remote STM and issues Time Attribute Certificate (TAC) that contains the results
- RTA plays the role of an Attribute Authority and issues X.509 compliant Attribute Certificates to attest to measurement results
- RTA acts like a Certificate Authority for time

Timestamping Solution

- RTA operates as a TTP with auditable practices and procedures
- RTA maintains traceability through multiple, redundant time sources and through measurement of its clocks by National Measurement Institutes (NMI)
- Timestamp consumers can operate their own STM and rely on RTA for traceability

Additional Research

- Implications, on a trusted system, of the uncertainty issues pertaining to the remote measurement of a clock over a network or the internet
  - Formally define security policies that incorporate the uncertainty of a measurement
- Clock trustworthiness and performance
  - Regardless of the level of precision, highly accurate and trustworthy time keeping with open up new avenues for the application of trusted time

Summary

- The forensic investigator must understand the issues regarding time integrity
- Secure Timestamping solutions are being adopted by industry
- Digital evidence integrity can be improved by the application of digital timestamps
- Additional research may yield significant advancements in trusted time keeping technology

Sources

1. Vanstone Scott A., Oorschot Paul C. van, Menezes, Alfred J. (1997) Handbook of Applied Cryptography, CRC Press
2. C. Adams, P. Cain, D. Pinkas, R. Zuccherato, “Internet X.509 Public Key Infrastructure Time-Stamp Protocol” RFC 3161, August 2001
3. NIST, “World Time Scales,” http://physics.nist.gov/GenInt/Time/world.html
4. Lombardi, Michael A., “Traceability in Time and Frequency,” NIST Time and Frequency Division Publication