

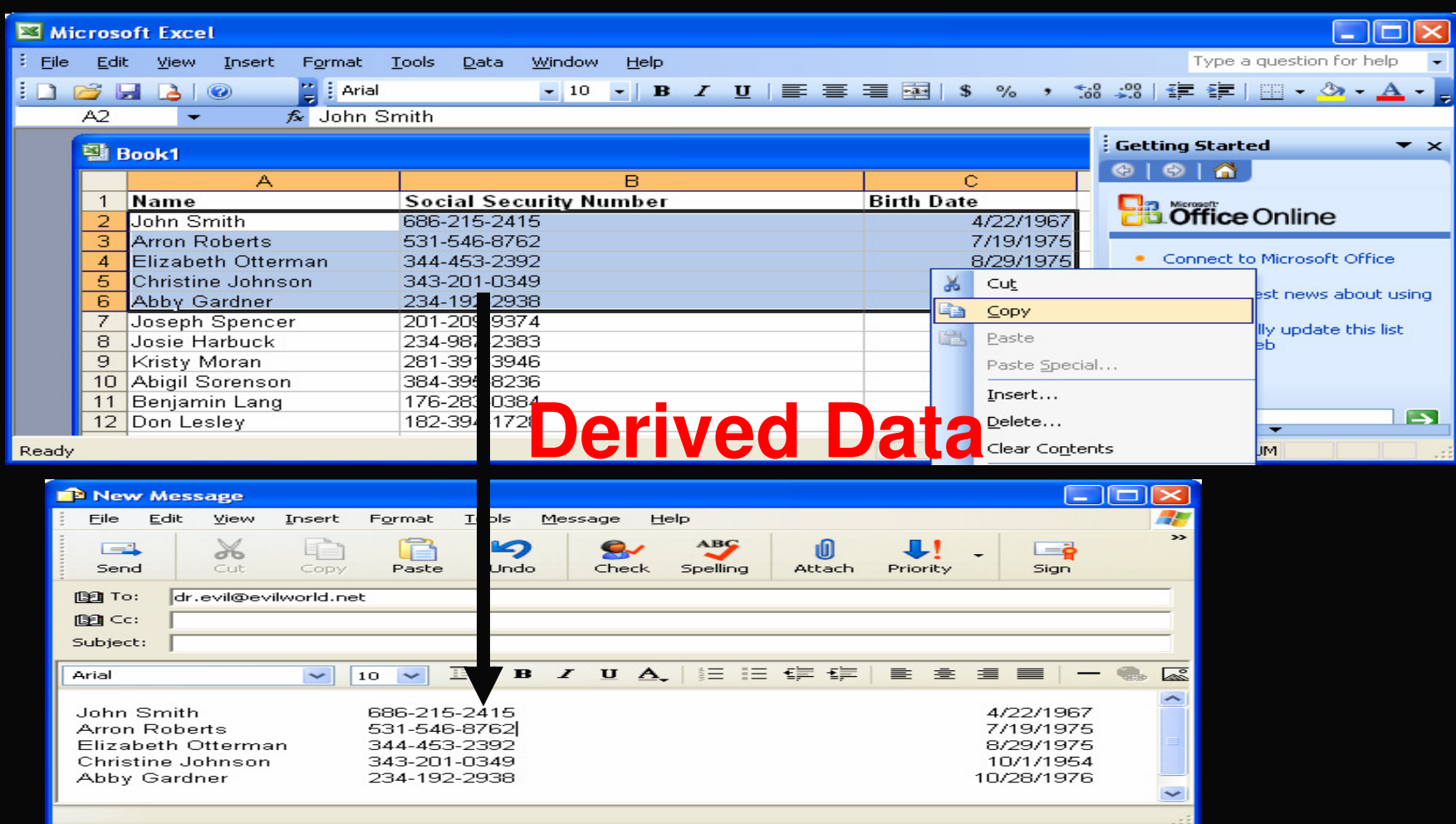
System Support for Derived Data Management

MOTIVATION

- Everyone has SENSITIVE data
- Releases are both advertent and inadvertent
- Affect customer confidence
- May cause regulatory compliance violations (HIPPA, FISMA, Sarbanes Ox, etc...)

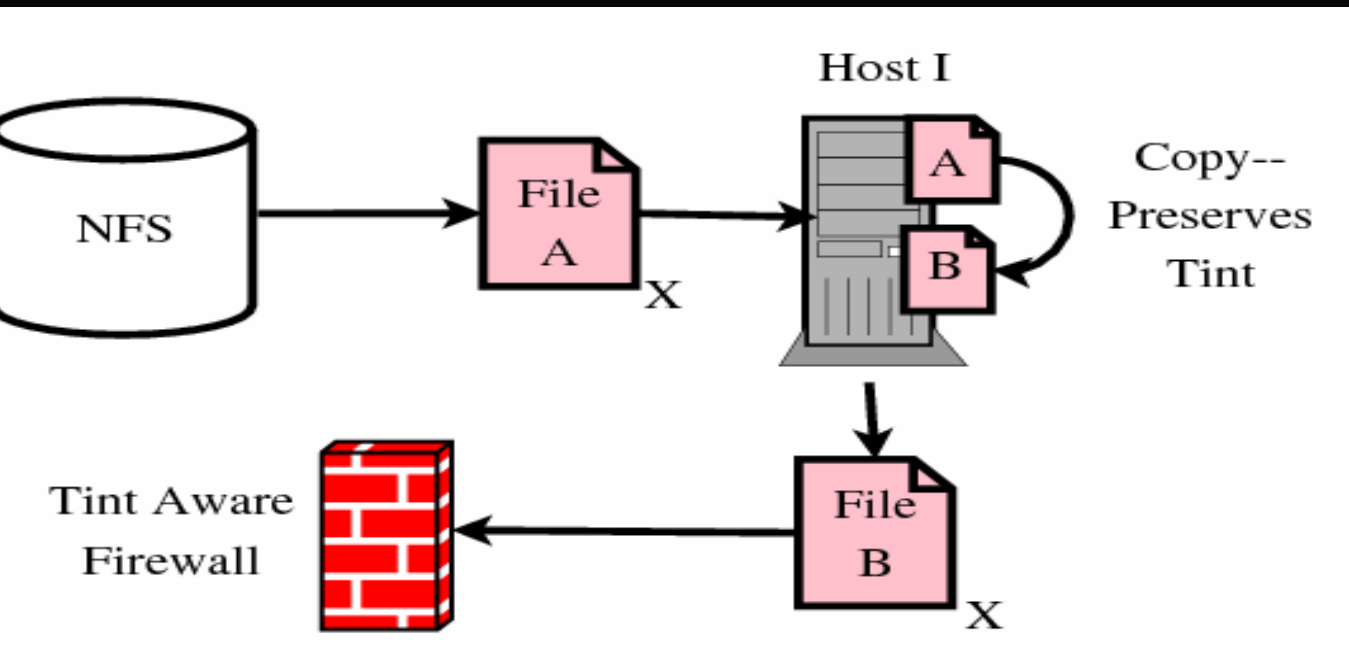


Example 1: copy and paste



NEON IN ACTION

- Experiment setup: Tints originate from NFS server.
- Hosts are run on trusted VMMs running modified Xen and Qemu.
- Our system actively combines tints and tracks derived data within the protected network

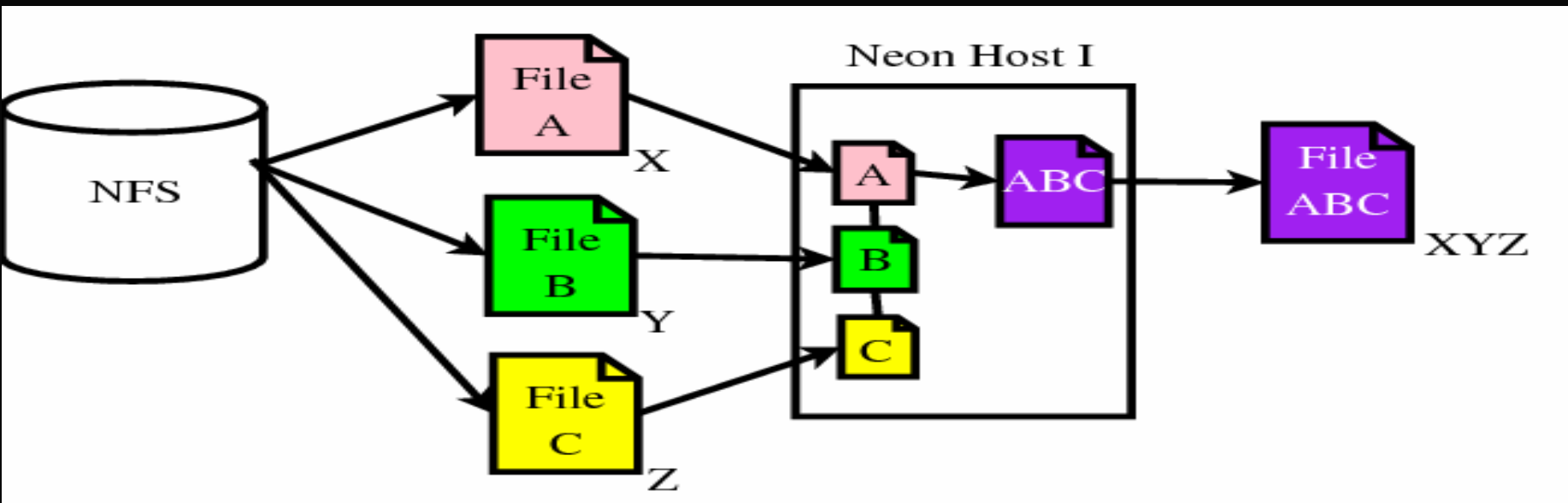


- Organizations want to enforce different policies on sensitive data
- For example:

- Access control
- Regulation of Data Flow
- To:
- Protect Trade secrets
- Regulate Constraints



Example 2: generated file i.e., from a compile



If file C is an object file compiled from source files A ,B ,C it will have an aggregated tint value.

The NFS is tint aware

i.e., if file A is tinted and B is derived from A, a copy or a compile, it will have the same tint values as A on the NFS server.

OUR SOLUTION: NEON

- Attribute data with a tint
- Monitor and Track dataflow on a single host
- Track dataflow within a protected network
- Propagate tints to derived data
- Operates Transparently
- Unmodified hosts as opposed to existing systems such as Asbestos and HiStar
- Fined grained Tracking
- Enforce policies based on tint values
- i.e. only allow encrypted I/O writes to disk

IMPLEMENTATION

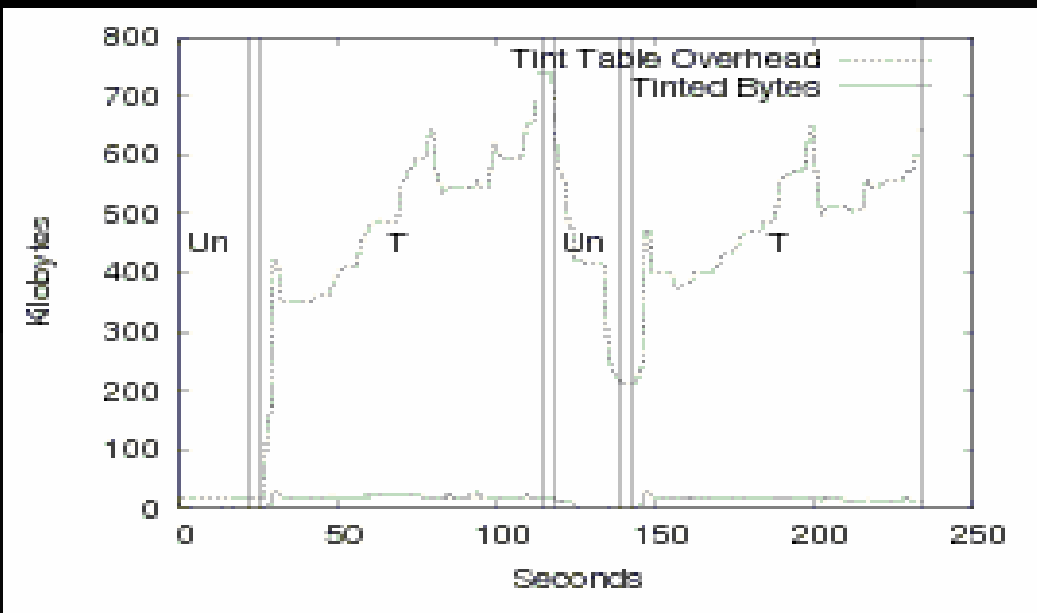
- Hosts run in our trusted VMM Xen
- Selectively trap into emulation i.e. when handling tinted data
- Emulator (Qemu)
- track tinted data movement
- aggregate different tints values
- Embed tint metadata into IP packets

Evaluation

- Close to no overhead in virtual mode
- Suffers a large overhead during emulation
- Provides exceptional forensics for tracking data

	Non-Qemu (s)	Qemu (s)	Tinted (s)	Space (MB)
Local Copy	0.010	0.011	0.098	0.86
Local Copy (2 tints)	0.010	—	0.055	0.73
Local Copy (4 tints)	0.010	—	0.081	1.14
Local Copy (8 tints)	0.010	—	0.100	1.62
Remote Copy	1.279	1.136	2.002	0.90
Remote Copy (2 tints)	1.243	—	4.535	0.84
Remote Copy (4 tints)	1.450	—	5.056	1.30
Remote Copy (8 tints)	1.237	—	4.882	1.88
Local Compress	0.087	0.082	8.346	0.85

Neon overhead processing 4 MB file



Memory used in compile test