Agenda for Misuse Detection Project Meeting: Monday 10-Feb-97, 10am-12pm

Select a timekeeper.

Equipment issues (0:15)
- HD for julie
- HD for notebook
- Backup
- Insurance
- more RAM for Gateway (32MB)
- Network Card (keep or return?)

Auditing base objects in NT 4.0 (0:10)

NT seminar (0:05)
- no news is good news

Julie's thesis proposal (0:15)

KDD talk (0:20)
- postponed

Healtheon letter (0:05)
- postponed

Topics for next agenda (0:05)

---

10-Feb-97 Meeting Notes

Attendees: Steven Templeton, Chris, Julie, Brant
Notes taken by Chris Wee
Meeting began @ 12:40pm and ended @ 1:30pm
Julie was the timekeeper

Installation of machines. (0:10)

Healtheon letter. (0:05)
Agenda for Misuse Detection Project Meeting: Monday 15-Apr-97, 6pm - 8pm

Select a timekeeper.
Have you kissed your IRS agent today?

Admin (0:05)
Oakland conference. everyone registered?
suggestion to move the meeting to 5:30pm - 7:30pm

Audit countermeasures (0:10) Brant, Chris
Brant has a seminar slot on 4/23 Wed 3pm. What is he planning to cover?

N-gram code (0:10) Steven
initial work plan?

blumfield UCDMC Matt & Steven
Matt and Steven have discussed the outline.
Slot is Sat 5/24, 1-2pm. Chris and Steven presenting.

UCD internal auditors (0:10) Chris
Chris met with David Day, UCD IA for 2.5 hours on 4/11.
Covered 11-step audit model
Reviewed manual application of model to Financial aid
Another meeting on Fri 4/18 9am, can bring 2 students
Another meeting with FBI, IT, IA, CS on 5/1 Matt & Chris attending
DaPIS, on-line accounting,
http://accounting.ucdavis.edu/docs/fis/fis.htm

Mentee industrial espionage (0:10) Chris
Maria has read the Ira Winkler paper, currently getting Donn Parker's books from the library. We can review transport of collected data, (review misuse model)

mike clifford (0:20) Julie
opinions?

2nd yr funding (0:20) Karl
When do we start talking about a proposal for additional funds. Assuming Jennifer and Susan have sue funds for a 2nd year of work, they will require a proposal from us. Assuming further that it is FY97 funds that they have set aside for the continuation, they will have to commit those funds by Aug at the latest.

ARCA report on data-driven attacks (0:10) Julie
our objective: formulate plan to re-create some experiments

Fannie Mae (0:20) Chris

15-Apr-97 Meeting Notes
Attendees: Steven Templeton, Chris, Julie, Brant, Karl
Notes taken by Chris Wee
Meeting began @ 12:16pm and ended @ 1:00pm

meeting on Mon 4/21,
our objective: give feedback on what topics you'd like to learn

Admin (0:10)
more RAM for Gateway (32MB) has this been installed?
Network Card came in about 1.5 weeks ago
//port Zip drive

Topics for next agenda (0:05)
Agenda for Misuse Detection Project Meeting: Monday 22-Apr-97, 6pm-8pm

Select a timekeeper.

Audit countermeasures (0:20) Brant

N-gram code (0:20) Steven

Initial work plan? timetable?

Blumfield UCDMC Matt & Steven

Matt and Steven have discussed the outline.

Slot is Sat 5/24, 1-2pm. Chris and Steven presenting.

The outline is...

Mentee industrial espionage (0:10) Julie

Julie met with Maria Lau and will supervise her

in writing a virus, possibly polymorphic.

2nd yr funding (0:20) Karl

Proposal for additional funds. Assuming Jennifer and Susan have not funds for a 2nd year of work,

they will require a proposal from us.

Assuming further that it is FY97 funds that they have set aside for the continuation,

they will have to commit those funds by Aug at the latest.

Debrief Fannie Mae (0:20) Chris

Meeting on Mon 4/21,

Debrief UCD IA meeting (0:00) Chris

Meeting was cancelled by David Day, UCD IA.

Steven reschedule.

Admin (0:10)

RAM for Gateway (32MB) was installed by David. Thanks David.

//port Zip drive

Atlantis

Julie's move into 2244

Topics for next agenda (0:05)

22-Apr-97 Meeting Notes

Attendees: Steven Templeton, Chris, Julie, Brant, Karl, Raymond
Agenda for Misuse Detection Project Meeting: Thursday 08-May-97, 5:30pm - 7:30pm

Select a timekeeper.

**Virus detection progress** (0:20) Julie — Jaz Drive, P.O. Norton & Dr. Solomon

**HP & Intel presentations** (0:10) Chris
  what we think they are interested in

**Oakland** (0:20) Chris
  are we equipped to perform BSM auditing?
  are we equipped to perform NT auditing?
  have Chris' tools been ported to NT?
  Brant, please summarize feedback from seminar

**UCD IA meeting** (0:10) Chris
  meeting was cancelled by David Day, UCD IA.
  Steven tried to reschedule.

**review OMG audit and security standards** (0:10) Chris

**Admin** (0:15)
  disk drives ordered?
  Toshiba sent back (not yet)
  //port Zip drive

**Topics for next agenda** (0:05)

---

08-May-97 Meeting Notes

Attendees: Steven Templeton, Chris, Julie, Brant(briefly)

Marianne Moller, JavaSoft

Time for auditor meeting.

Report on polymorphism on a macro virus.