File 20100422.1256: This is what I sent to John Lyle earlier today:

Dear John,

A citable reference is the chapter 'A History of Computer Security Standards' by Jeffrey R. Yost, in The History of Information Security: A Comprehensive Handbook, ed. by Karl de Leeuw and Jan Bergstra. Elsevier, 2007. The book is in the comlab library. I have a copy at home since I can't get there right now. Chapter 20 describes Willis Ware and the early (mid 1960s) notice that NSA took of the security problems introduced by time sharing.

I searched through my BibTeX file and could not find any papers from the 1940s or 1950s mentioning information security. It hadn't been thought of yet, aside from Bletchley Park's work during the 1940s, and that remained classified until 1979. The first conference mentioning computer security was in 1967 (Proceedings of the Spring Joint Computer Conference, Atlantic City, New Jersey, April 18--20, 1967). In the very early 20th century, WWI signal corps members knew that telegraph lines and field telephones could be eavesdropped, but they didn't publish about it in the open literature. Computer security appeared in the open literature in 1967 (Ware, 1967). Interestingly, it was in the biomedical applications track because there wasn't a track for infosec yet.

Now, going back a ways, information (not computer) security---primarily secret writing and optical telegraphs, viz. people waving semaphore flags atop towers---was most clearly written about by the Right Reverend Sir John Wilkins. A few earlier writers had written about secret writing, but Trithemius (1499) for example buried all the content so deep in talk of demons and angels and magic that it took a century after his death before anyone figured out what he was talking about.

John Wilkins wrote in 1641 of the need for objective validation (rather than appeal to Magick) of IA systems in Chapter XIX of his book. I think it's the first solid mention of information security. I confess that Ross Anderson told me of this book's existence, but I went and read the whole book in the Bodleian, and it's well worth an afternoon. There was much more in there than Prof. Anderson told me.

Wilkins was different from earlier writers. Whereas Trithemius was a theologian and risked his job if he were to be found messing around with occult knowledge (hence his careful couching of all the terminology in terms of angels and evil), and Francis Godwin made the claim that a method existed for 'detecting all Lying and falsehood' but didn't say how, Wilkins not only showed how security worked, but how it breaks. Immediately following a complete tutorial on cryptography, he presented a short course in cryptanalysis. He talked about how to measure accuracy in communication channels. Wilkins was undoubtedly aware of Mary Queen of Scots' catastrophe a decade or so earlier due to poor information security (although he refers to it only obliquely). He mentions the full disclosure debate and also the risk of coming to the attention of the authorities if you're caught doing too much research in this area. Reading his book in Duke Humphrey's library was fun. Well-written, funny in spots, and it rang all sorts of bells in my mind.

Wilkins did his undergraduate degree in Arts at Magdalen Hall, Oxford; later he became Warden of Wadham College, then Head of Trinity College in Cambridge. After the Restoration of Charles II, he was run out of Cambridge, then became one of the founders of the Royal Society in London.

References:

```
@inproceedings{Ware1967,
    author = {Willis H.~Ware},
    title = {Security and privacy in computer systems},
    booktitle = {Proceedings of the Spring Joint Computer Conference},
    address = {Atlantic City, New Jersey},
    pages = {279--282},
    year = 1967,
}

@book{Wilkins1641,
    author = {John Wilkins},
    title = {Mercvry, or the Secret and Swift Messenger: Shewing, How a Man may with Privacy and Speed communic
    publisher = {Printed by I.~Norton, for Iohn Maynard, and Tomothy Wilkins, and are to be sold at the George
    address = {London},
    year = 1641,
    note = {Located in Duke Humphrey's library at the Bodleian},
}

@book{Trithemius1499,
    title = {Steganographia},
    author = {Trithemius, Johannes},
    year = 1499,
    publisher = {Darmbstadii},
    note = {\it Ex officina typographica Balthasaris Aulandri, sumptibus ver Ioannis Berneri, bibliop.\ Francof
}

@book{Trithemius1606,
    author = {Johannes Trithemius},
    title = {\it Steganographia: Hoc est: Ars per occvltum scritorum animi svi volvntatem absentibvs aperiendi
    publisher = {Frankfurt},
    year = 1606,
}

@book{Trithemius1608,
    author = {Johannes Trithemius},
    title = {\it Steganographia: Hoc est: Ars per occvltam scriptvram animi svi volvntatem absentibvs aperiendi
    publisher = {Francofvrti},
    year = {M.~DC.~VIII},
}

@book{Trithemius1564,
    author = {Johannes Trithemius},
    title = {\it Polygraphiae Librae Sex: Ioannis Trithemii Abbatis Peapolitani, quondam Spanheimensis, ad Maxi
    publisher = {\it Coloni: apud Ioannem Birckmannum \& Wernerum Richwinum},
    year = 1564,
    note = {Located in the Christ Church College spec.\ coll.},
}

I hope this helps.  I have more details if you want them, but it's in
narrative form in my (not very long yet) draft dissertation.  Can you
cite a dissertation that hasn't been finished yet?  That's why I gave
you primary sources above, so you can cite those.

Joe Loughry
Doctoral student in the Computing Laboratory
St Cross College, Oxford
----------------------------------------
From: John Lyle [john.lyle@keble.ox.ac.uk]
Sent: 22 April 2010 14:35
To: Joe Loughry
```

```
Subject: Reference

Hi Joe,

I hope all is well.  I was wondering if I could take advantage of your
enormous knowledge of system certification / assurance literature?  I'm
after a reference that shows just how long system assurance methods have
existed ... I've got a (rather bland, admittedly) statement in my
literature review that I would like to support:

"The need to assess and evaluate the trustworthiness (and security) of
computing platforms has been around for nearly as long as computing
platforms themselves~\cite{??}"

I'm trying to reassure the reader that I'm not naively presenting my
dissertation as the first attempt at establishing software trustworthiness!

Any terrifically old or classic references would be much appreciated.
I've got (and read) some, but I wondered if you knew of a definitive
reference.  I remember you citing books from the 16th(?) century in your
transfer report, so thought you might be the person to ask!

Thanks,

John
```

References