



MAX PLANCK INSTITUTE
FOR SECURITY AND PRIVACY

IT-Sicherheit der Zukunft: Danke für Ihr Vertrauen

Peter Schwabe

6. November, 2024

FORBES > INNOVATION > CYBERSECURITY

AI Is The Past, Present And Future Of Cybersecurity

EMERGING TECHNOLOGIES

Cybersecurity is on the frontline of our AI future. Here's why

Cyber AI: Real defense

Augmenting security teams with data and machine intelligence

Microsoft Copilot for Security

Protect at the speed and scale of AI with a generative AI-powered assistant—announcing Copilot for Security general availability.

Contact Sales

PUTTING THE AI IN URANIUM

MICROSOFT NEEDS SO MUCH POWER TO TRAIN AI THAT IT'S CONSIDERING SMALL NUCLEAR REACTORS

IT'S A HIGHLY AMBITIOUS PLAN.

Google to Power AI Data Centers with Nuclear Energy



by Technology Journalist
Franklin Okeke

Fact Checked by
Duncan Proctor

Updated on
15 October 2024







0 3.68k Share

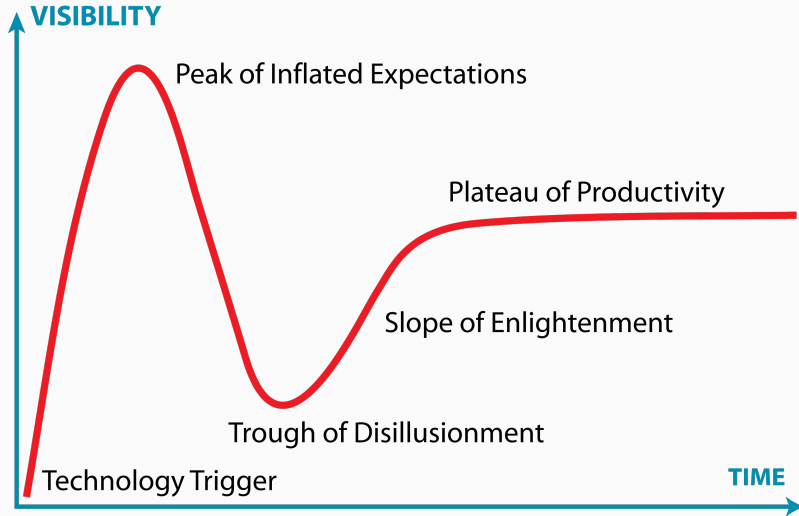
Democracy for the 21st Century: Using Blockchain to Revitalize Our Governments

by Teresa Lu-Romeo August 18, 2021 Summer 2021 Fellowship

The New York Times

Bitcoin Uses More Electricity
Than Many Countries. How Is
That Possible?

Hype-Zyklen



Wie erkennt man einen Hype?

- Gefühlt 90% aller Vorträge drehen sich (teilweise) um KI/ML
- Aktionismus der Politik
- Forschungsförderung für die Nutzung einer Technologie, nicht für die Lösung eines konkreten Problems
- Unsummen Venture Capital sind im Spiel
- Experten warnen vor überzogenen Versprechen

Das ist nicht unbedingt schlecht!

- Deutlicher Fortschritt der Forschung
- Wir lernen jede Menge über eine (neue) Technologie
- Das Plateau ist typischerweise höher als der Anfangspunkt
- Man lernt auch (schmerzhaft), was nicht geht

Trusted

- Darf nicht kaputtgehen
- Darf nicht böseartig werden
- Reißt andere Komponenten mit in den Abgrund
- Typischerweise hohe Privilegien

Trustworthy

- Klar definierte Sicherheitseigenschaften
- Klar definiertes Angreifermodell
- Systematisch sicher gebaut
- Idealfall: formal verifiziert
- Sorgfältig studierte Annahmen

Trusted

- Darf nicht kaputtgehen
- Darf nicht böartig werden
- Reißt andere Komponenten mit in den Abgrund
- Typischerweise hohe Privilegien

Trustworthy

- Klar definierte Sicherheitseigenschaften
- Klar definiertes Angreifermodell
- Systematisch sicher gebaut
- Idealfall: formal verifiziert
- Sorgfältig studierte Annahmen

Sichere Systeme

1. Trenne *trusted* Komponenten sauber von dem Rest.
2. Stelle sicher, dass alle *trusted* Komponenten auch *trustworthy* sind.

Wir *vertrauen* Hype Technologie bevor sie auch nur die Chance hat vertrauenswürdig zu werden!

Saubere Trennung ist schwer

- Sicherheit trifft auf Workflows
- Saubere Trennung muss UX einbeziehen

Saubere Trennung ist schwer

- Sicherheit trifft auf Workflows
- Saubere Trennung muss UX einbeziehen
- Zu starke Trennung wird nicht akzeptiert
- Zu schwache Trennung erfordert aufwendigere
 - Formalisierung der Interfaces
 - Annahmen

Saubere Trennung ist schwer

- Sicherheit trifft auf Workflows
- Saubere Trennung muss UX einbeziehen
- Zu starke Trennung wird nicht akzeptiert
- Zu schwache Trennung erfordert aufwendigere
 - Formalisierung der Interfaces
 - Annahmen

Vertrauenswürdige Komponenten sind teuer

- Beispiel: High-assurance Kyber (ML-KEM)
 - Beginn des Projekts: Februar 2020
 - Paper in 2023 und 2024 mit je ≥ 14 Autoren
 - Software weitestgehend "fertig", noch nicht im Einsatz

Wer trifft Entscheidungen?

Nutzer

- Will dass Technologie *einfach* funktioniert
- Will dass Technologie billig ist
- Will Features
- Findet Sicherheit schon irgendwie wichtig, aber nur
 - Wenn es (fast) nichts kostet
 - Wenn man es (fast) nicht bemerkt

Wer trifft Entscheidungen?

Nutzer

- Will dass Technologie *einfach* funktioniert
- Will dass Technologie billig ist
- Will Features
- Findet Sicherheit schon irgendwie wichtig, aber nur
 - Wenn es (fast) nichts kostet
 - Wenn man es (fast) nicht bemerkt

Management

- Will sichere IT Systeme haben. . .

Wer trifft Entscheidungen?

Nutzer

- Will dass Technologie *einfach* funktioniert
- Will dass Technologie billig ist
- Will Features
- Findet Sicherheit schon irgendwie wichtig, aber nur
 - Wenn es (fast) nichts kostet
 - Wenn man es (fast) nicht bemerkt

Management

- Will sichere IT Systeme haben. . .
- . . . aber sich am liebsten nicht drum kümmern
- Leider zu oft "CMA Mentalität"

Wer trifft Entscheidungen?

Nutzer

- Will dass Technologie *einfach* funktioniert
- Will dass Technologie billig ist
- Will Features
- Findet Sicherheit schon irgendwie wichtig, aber nur
 - Wenn es (fast) nichts kostet
 - Wenn man es (fast) nicht bemerkt

Management

- Will sichere IT Systeme haben. . .
- . . . aber sich am liebsten nicht drum kümmern
- Leider zu oft “CMA Mentalität”
- “Sicherheit” nur mit Windows und Outlook

Es ist alles noch viel schlimmer

- Vertrauenswürdige Komponenten machen Annahmen
 - darüber wie sie genutzt werden
 - **darüber was sie nutzen**

Es ist alles noch viel schlimmer

- Vertrauenswürdige Komponenten machen Annahmen
 - darüber wie sie genutzt werden
 - **darüber was sie nutzen**
- Beispiele für zu optimistische Annahmen:
 - Faktorisierung ist schwer

Es ist alles noch viel schlimmer

- Vertrauenswürdige Komponenten machen Annahmen
 - darüber wie sie genutzt werden
 - **darüber was sie nutzen**
- Beispiele für zu optimistische Annahmen:
 - Faktorisierung ist schwer
 - Spectre Angriffe. . .

Es ist alles noch viel schlimmer

- Vertrauenswürdige Komponenten machen Annahmen
 - darüber wie sie genutzt werden
 - **darüber was sie nutzen**
- Beispiele für zu optimistische Annahmen:
 - Faktorisierung ist schwer
 - Spectre Angriffe. . .
 - Optimierung von Compilern

Es ist alles noch viel schlimmer

- Vertrauenswürdige Komponenten machen Annahmen
 - darüber wie sie genutzt werden
 - **darüber was sie nutzen**
- Beispiele für zu optimistische Annahmen:
 - Faktorisierung ist schwer
 - Spectre Angriffe. . .
 - Optimierung von Compilern
 - Pager-Angriff gegen Hisbollah

Aber es geht eine Menge, wenn man will

- seL4: formal verifizierter Microkernel
 - Genutzt, z.B. in Automobil- und Luftfahrtindustrie

Aber es geht eine Menge, wenn man will

- seL4: formal verifizierter Microkernel
 - Genutzt, z.B. in Automobil- und Luftfahrtindustrie
- HACL*: Formal verifizierte Kryptographie
 - Genutzt, z.B. in Firefox

Aber es geht eine Menge, wenn man will

- seL4: formal verifizierter Microkernel
 - Genutzt, z.B. in Automobil- und Luftfahrtindustrie
- HACL*: Formal verifizierte Kryptographie
 - Genutzt, z.B. in Firefox
- Formosa Crypto: Formal verifizierte Kryptographie
 - Sicherheit auch gegen Spectre Angriffe

Aber es geht eine Menge, wenn man will

- seL4: formal verifizierter Microkernel
 - Genutzt, z.B. in Automobil- und Luftfahrtindustrie
- HACL*: Formal verifizierte Kryptographie
 - Genutzt, z.B. in Firefox
- Formosa Crypto: Formal verifizierte Kryptographie
 - Sicherheit auch gegen Spectre Angriffe
- Cheri: Sicherheitsorientierte CPU Erweiterungen
 - Erweiterungen für Risc-V und Arm ("Morello")

Aber es geht eine Menge, wenn man will

- seL4: formal verifizierter Microkernel
 - Genutzt, z.B. in Automobil- und Luftfahrtindustrie
- HACL*: Formal verifizierte Kryptographie
 - Genutzt, z.B. in Firefox
- Formosa Crypto: Formal verifizierte Kryptographie
 - Sicherheit auch gegen Spectre Angriffe
- Cheri: Sicherheitsorientierte CPU Erweiterungen
 - Erweiterungen für Risc-V und Arm ("Morello")
- OpenTitan: Open-source HW "root of trust"
 - Erfolgreiches Tapeout Anfang 2024

Aber es geht eine Menge, wenn man will

- seL4: formal verifizierter Microkernel
 - Genutzt, z.B. in Automobil- und Luftfahrtindustrie
- HACL*: Formal verifizierte Kryptographie
 - Genutzt, z.B. in Firefox
- Formosa Crypto: Formal verifizierte Kryptographie
 - Sicherheit auch gegen Spectre Angriffe
- Cheri: Sicherheitsorientierte CPU Erweiterungen
 - Erweiterungen für Risc-V und Arm ("Morello")
- OpenTitan: Open-source HW "root of trust"
 - Erfolgreiches Tapeout Anfang 2024
- Qubes OS: Trennung durch konsequente Virtualisierung
 - Mein Produktivsystem seit 8 (?) Jahren
 - Top of my Wunschliste: Formal verifizierter Hypervisor

A propos Wunschliste

Ich wünsche mir...

- dass wir Technologie nicht vertrauen, bevor sie vertrauenswürdig ist

A propos Wunschliste

Ich wünsche mir...

- dass wir Technologie nicht vertrauen, bevor sie vertrauenswürdig ist
- ... und erst recht nicht bevor wir überhaupt wissen, was es heißt vertrauenswürdig zu sein!

Ich wünsche mir...

- dass wir Technologie nicht vertrauen, bevor sie vertrauenswürdig ist
- ... und erst recht nicht bevor wir überhaupt wissen, was es heißt vertrauenswürdig zu sein!
- mehr Forschung an
 - offenen, nutzbaren Ansätzen zum sauberen Trennen von Komponenten
 - offener vertrauenswürdiger Technologie
 - der Validierung weit-akzeptierter Annahmen

Ich wünsche mir...

- dass wir Technologie nicht vertrauen, bevor sie vertrauenswürdig ist
- ... und erst recht nicht bevor wir überhaupt wissen, was es heißt vertrauenswürdig zu sein!
- mehr Forschung an
 - offenen, nutzbaren Ansätzen zum sauberen Trennen von Komponenten
 - offener vertrauenswürdiger Technologie
 - der Validierung weit-akzeptierter Annahmen
- dass wir lokal IT-Sicherheitskompetenz bilden und erhalten

Ich wünsche mir...

- dass wir Technologie nicht vertrauen, bevor sie vertrauenswürdig ist
- ... und erst recht nicht bevor wir überhaupt wissen, was es heißt vertrauenswürdig zu sein!
- mehr Forschung an
 - offenen, nutzbaren Ansätzen zum sauberen Trennen von Komponenten
 - offener vertrauenswürdiger Technologie
 - der Validierung weit-akzeptierter Annahmen
- dass wir lokal IT-Sicherheitskompetenz bilden und erhalten
- dass etwas mehr auf Experten gehört wird

Ich wünsche mir...

- dass wir Technologie nicht vertrauen, bevor sie vertrauenswürdig ist
- ... und erst recht nicht bevor wir überhaupt wissen, was es heißt vertrauenswürdig zu sein!
- mehr Forschung an
 - offenen, nutzbaren Ansätzen zum sauberen Trennen von Komponenten
 - offener vertrauenswürdiger Technologie
 - der Validierung weit-akzeptierter Annahmen
- dass wir lokal IT-Sicherheitskompetenz bilden und erhalten
- dass etwas mehr auf Experten gehört wird

Ja, das ist eine langweilige Idee für die Zukunft der IT-Sicherheit, aber ich hatte Sie gewarnt.

Danke für Ihr Vertrauen