

# Monocultures and Diversity in IT

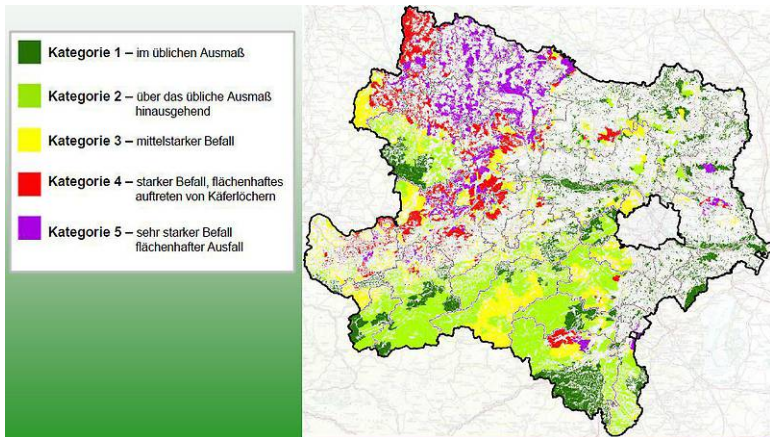
Dr. Johanna Ullrich  
SBA Research  
jullrich@sba-research.org



<https://noe.orf.at/v2/news/stories/2965733/>



<https://www.n-tv.de/wissen/Experte-Borkenkaefer-schnell-bekaempfen-article19926717.html>



<https://noe.orf.at/stories/3003854/>

If you become a monoculture,  
you are at great risk of perishing.

Georg M. Church

# Monocultures

# 2014: Heartbleed



<http://heartbleed.com/>

# 2014: Heartbleed

SERVER, ARE YOU STILL THERE?  
IF SO, REPLY "HAT" (500 LETTERS).



User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long". User Karen wants to change account password to "C0tt0r3st" User



HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "C0tt0r3st" User

User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about snakes but not too long". User Karen wants to change account password to "C0tt0r3st" User



<http://heartbleed.com/>



# OpenSSL

2014: 55 %

Z. Durumeric et al. "The Matter of Heartbleed". IMC. 2014.

# OpenSSL

2014: 55 %

Z. Durumeric et al. "The Matter of Heartbleed". IMC. 2014.

2017:

# OpenSSL

2014: 55 %

Z. Durumeric et al. "The Matter of Heartbleed". IMC. 2014.

2017: 84 %

M. Nemecek et al. "Measuring Popularity of Cryptographic Libraries in Internet-Wide Scans". ACSAC. 2017.

# 2016: Mirai

# 2018: Meltdown/Spectre



<https://meltdownattack.com/>

If you become a monoculture,  
you are at great risk of perishing.

Georg M. Church

# Diversity



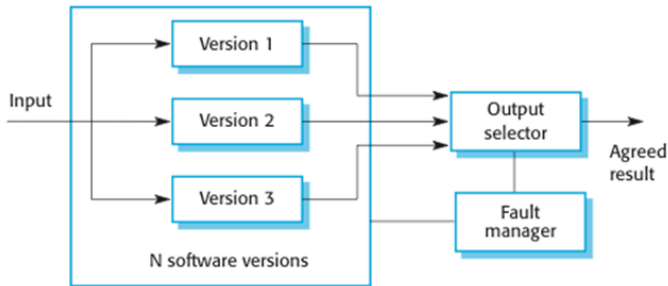
<https://www.n-tv.de/wissen/Experte-Borkenkaefer-schnell-bekaempfen-article19926717.html>





<https://www.br.de/themen/wissen/wald-lebensraum-bayern112.html>

# Design Diversity (N-Version Programming)



[http://csis.pace.edu/~marchese/SE616\\_New/Sum\\_13/Sum\\_13.htm](http://csis.pace.edu/~marchese/SE616_New/Sum_13/Sum_13.htm)



<https://www.airbus.com>

**OpenSSL**  
Cryptography and SSL/TLS Toolkit

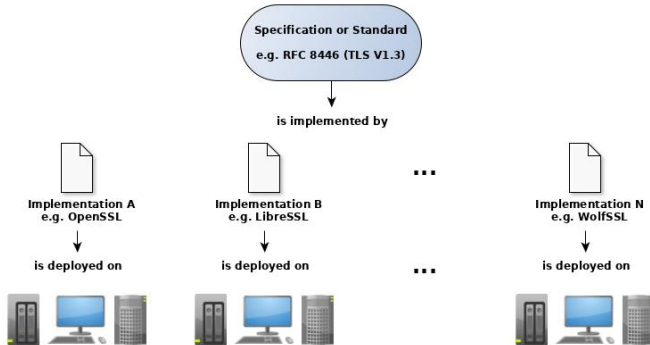
BoringSSL



Bouncy Castle



# Inherent N-Version Programming



# From theory to practice

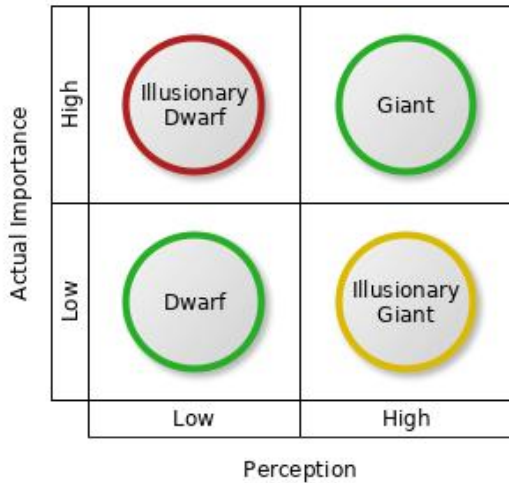
# Open Questions

1. Which technologies are used on the Internet?
2. How is diversity on the Internet determined?
3. Which strategies might lead to a more diverse Internet?

# Open Questions

1. Which technologies are used on the Internet?
2. How is diversity on the Internet determined?
3. Which strategies might lead to a more diverse Internet?





# Open Questions

1. Which technologies are used on the Internet?
2. How is diversity on the Internet determined?
3. Which strategies might lead to a more diverse Internet?

# Open Questions

1. Which technologies are used on the Internet?
2. How is diversity on the Internet determined?
3. Which strategies might lead to a more diverse Internet?



<https://unsplash.com>

# Monocultures and Diversity in IT

Dr. Johanna Ullrich  
SBA Research  
[jullrich@sba-research.org](mailto:jullrich@sba-research.org)